The Professional Identity of Security Risk Intelligence Analysts in the Private Sector: an International Perspective

Magdalena Adriana (Dalene) Duvenage

UP841301

University of Portsmouth

Institute of Criminal Justice Studies

The thesis submitted in partial fulfilment of the requirements for the award of the degree of Professional Doctorate in Security Risk Management of the University of Portsmouth

April 2021

Declaration

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award.

Word count: 50,074

(Excluding tables, graphics, bibliography and appendices)

Table of contents

List of tables

Chapter 4

Chapter 5

List of Figures

Chapter 2:

Chapter 3:

Chapter 4:

Chapter 5:

Abstract

This study aims to contribute to the understanding of the emerging profession of Security Risk Intelligence Analysis in the private sector by exploring the individual and collective professional identity of practitioners who identify and analyse threats and risks to the security of personnel, key assets and operations of an organisation or business in the private sector. The study used a mixed-method approach for the empirical research of how practitioners across different organisational contexts and national boundaries construct and maintain their professional identity in their quest for meaningful work.

Security risk intelligence analysts in the private sector share the same individual professional identity, forming the collective professional identity's blueprint. There were some elements of difference, but none of them impacted the overall results that emerged during the study. Their professional identity is centred on their expert knowledge and ability to perform complex intellectual tasks in providing forewarning and insight into threats to the organisation or client's well-being and sustainability. They have a strong individual professional identity that reflects high levels of job satisfaction, pride and autonomy in their profession who thrive on connecting on a professional, functional level with stakeholders. Their main professional challenge related to the relative lack of understanding of their role in the private sector by various stakeholders in and outside the organisation.

Lastly, proposals are made on how the profession as a collective and individual security risk intelligence analysts can increase their professional identity and their concomitant impact on the security risk management field and the security sector.

Chapter 1

Introduction

1.1 Rationale

The growing diversity of threats, ranging from physical, criminal, political to cyber threats, impact all aspects of the well-being of countries, communities, the public and businesses. The latter, and specifically those organisations that established their own internal security risk or intelligence functions to manage these threats better, or provide these services to other companies in the last 20 years, is the broad context of this study. Zimmerman (2011) explains how businesses felt the need to act to understand better and manage the "coalsescing, new riskscape":

> Historic shifts in the geo-strategic environment and the attendant fragmentation of previously monolithic security risks into numerous, interdependent challenges, a change in perspective with regard to the added value of threat and risk analysis for internationally active businesses has, indeed, become a prerequisite for successful operations. As is true for almost everything regarding security issues, knowledge—particularly informational and intelligence superiority—plays a decisive role.

This *threat and risk analysis* and the resultant *security knowledge or intelligence*—and specifically the practitioners that execute this function—is the focus of this study. Due to the lack of a standardised job title for those performing this function, this study used the term "security risk intelligence analyst" (henceforth SRIA).

This study aims to shed some light on the socio-professional profile and expertise of the SRIA in the private sector across the globe by exploring both their individual and collective professional identities. More specifically, the research explored how these practitioners perceive their professional roles, overcome challenges they face, strengthen their motivation to remain in this specific career, and express their collective 'belonging' to an emerging, atypical profession.

Security risk intelligence analysis is an "emerging" profession. It emerged from the changes mentioned above in society and specifically the need for businesses to better understand and manage security threats. This created a new labour market for individuals who have either done this function before in government and law enforcement or newcomers drawn by the novel application of knowledge, skills and technology in the business environment.

Knowledge of intelligence analysts in the government sector has grown in the last few years, focusing on their professionalisation and the field of intelligence studies being accepted as a sub-discipline of security studies (Corvaja, Jeraj & Borghoff, 2016). However, very little is known of these practitioners in the private sector. They have not yet been studied, and very little is known about their function and professional identity, other than they "proactively identify, assess and communicate risks facing the company's personnel, facilities, information assets and operations, sometimes locally, but more often also on an international level" (Bode, 2016).

The study of Professional Identity is important because it explains the direction of the development and establishment of a profession and the factors that help shape it (Levin-Rozalis & Shochot-Reich, 2009). Although there is no agreed definition of professional identity among scholars, this study will define individual professional identity—"Who am I as a Security Risk Intelligence Analyst?"—to mean that self-conception or self-image based on skills, abilities, experiences and identification with a profession. Collective professional identity refers to a sense of unity among the professionals, possessing personal responsibility to the profession, conducting oneself ethically and morally, and experiencing feelings of pride for the profession (Alves & Gazzola, 2011). This collective professional identity–"Who are *we* as Security Risk Intelligence Analysts?"—means the shared or collective self-identification and framing with others in a specific profession.

A poorly developed or defined professional identity could harm the individual's search for meaningfulness, his job satisfaction, individual behaviour, functional duties, professional development, as well as services rendered to, and his relationship with

clients (Caza & Creary, 2016). In a security context, a poorly developed or identified professional identity could not only inhibit individual professional growth but could also have disastrous consequences when emerging threats are not detected, thereby causing real and reputational damage to the company or harm to employees, customers or the general public. Although this sociological construct has been well researched in the disciplines of education, organisational development, social work, and healthcare, none has been done in the whole of the intelligence analysis domain. There was no focus on analysts, as previous research only focused on the professionalism of operational personnel in private military companies (Franke & Von Boemcken, 2009; Schaub & Franke, 2009).

Using a pragmatist paradigm, this "profiling" of SRIA in the private sector will help understand how professional identity is created in new and emerging professions, especially where practitioners engage in divergent and multiple professional activities. For the first time, this study will give them a voice to tell how they perceive their professional roles, overcome challenges they face, strengthen their motivation to remain in this specific career, and express their collective 'belonging' to an emerging, atypical profession.

1.2 Research aims

In this ambiguous context, this study aims to understand the professional identity of SRIA's in the private sector. It will have a dual purpose: to explore 1) individual professional identity (their self-description in relation to performing an occupational role) and 2) the collective professional identity (the shared narrative with others who perform the same occupational role) by determining how the profession is perceived and constructed by those working within it.

The following two primary research questions will guide the study:

1. What is the individual SRIA's professional identity?
2. Is there a shared or collective professional identity among SRIA across organisational contexts and national boundaries, and if so, how does it manifest?

To achieve a better understanding of the lived experience of SRIA in the private sector, the following secondary research questions will illuminate our understanding of this emerging profession and its professional identity:

1. What is the self-perceived role, function and uniqueness of SRIA in the private sector?
2. How do intelligence analysts conceptualise or define their professional identity, and how do they perceive the profession?
3. What experiences and conditions does SRIA perceive as contributing to or strengthening their professional identities?
4. What experiences and conditions does SRIA perceive as hindering their professional identity? How do they renegotiate elements of their professional identity to overcome these challenges?
5. How do SRIA believe others perceive them?
6. What are their professional values and beliefs?

This study will use sociology theories, including social identity theory (Ashforth & Mael, 1989) and self-categorisation theory (Turner & Reynolds, 2012) on both an individual and group level to understand SRIA' affinity with their profession better. The data will be collected through two instruments, a web survey and semi-structured interviews. The survey placement in an international context will provide a valuable opportunity to collect, analyse and compare the perceptions and opinions of a completely under-researched group of practitioners on these matters. The multi-national sample will enable useful comparisons across national and organisational settings and ascertain whether professional identities transcend national and organisational contexts. The in-depth interviews with several security risk intelligence analysts will give a window on their lived experience in this profession.

The research results should be useful to practitioners themselves who will critically reflect on the essence or current state of their profession and its future. The study identifies the factors that help shape this emerging profession and provides practitioners with a platform to create self-awareness and articulate their strengths and potential contribution to the broader security and intelligence disciplines. Decision-

makers in both the private and public sector would find it useful to understand the potential benefits of intelligence led-security and how practitioners view the value they bring to the security and intelligence industry. Educators and professional development specialists could use the findings to develop new intelligence and security risk curricula while training programmes could be improved to make them more effective and fit-for-purpose. Human resources consultants should be able to use the results to improve their job profiles and improve career development initiatives to strengthen analysts' professionalism. Professional organisations would also be able to evaluate the most appropriate ways to strengthen the collective identity of SRIA.

1.3 Structure of the thesis

Chapter 2 will review the literature relevant to the professional identity of SRIA, drawing on several social identity theories to understand the professional identity construct, the context of the current private security risk industry and the function of these practitioners in this emerging professional field. The review will conclude with a summary and outline the aims and rationale of the present study.

Chapter 3 will present the interpretivist epistemology and exploratory pragmatic mixed method that was used in the study. An exploratory web survey was used to explore how the profession is perceived and constructed by those practising within the field. Sequential to this data collection, qualitative interviews aimed to provide an in-depth analysis of the lived professional experience of nine participants from four different countries and organisational contexts using the principles and methodology of Interpretative Phenomenological Analysis (IPA).

Chapters 4 and 5 will present the results of the web survey and IPA study in their entirety. Each chapter will include an abstract, introduction and rationale for the choice of method, a detailed account of the recruitment, data collection, management and analysis procedures, results, discussion and conclusion.

Chapter 6 will summarise and integrate the findings of the empirical studies presented in this thesis. This general discussion will also include implications from this work for

security risk intelligence analysis practice, provide directions for future research and draw conclusions from the work.

Chapter 2

Literature review

2.1 Introduction

The purpose of this review is to explore the existing literature on concepts, models and theories that relate to the professional identity of SRIA in the private sector. This chapter will first discuss the search strategy used for the study before moving on to the various disciplines that relate to the research topic. These disciplines or study areas are sociology and psychological sociology, private security, intelligence analysis and organisational studies (to a lesser degree). The review will conclude with a summary and outline the aims and rationale of the study.

2.2 Literature search strategy

The researcher found Ashforth's (2016) comment that "identity and identification are root constructs that bridge levels of analysis, levels of self, and multiple disciplines, they continue to generate a dizzying array of exciting and important research avenues" to be true when an inductive approach to the literature search strategy was followed since there is no existing literature on the specific research topic. The inductive approach's purpose was to explore the four different subject areas and then find the nexus between them to answer the research questions.

This exhaustive coverage approach (Randolph, 2009) made the literature research process laborious and lengthy. At the height of the collection phase, about 1500 different sources in the database were reduced to a third of that for the literature review and 170 sources for use in the methodology and subsequent chapters of the thesis. The search strategy focused mainly on the Portsmouth University Library's Discovery Service, which is a portal from where over 100 databases can be accessed, EBooks, British Library Ethos services, while Google Scholar, Google Books and ProQuest offered

a starting point to define the parameters of the literature search strategy. Mendeley was used as a reference and repository tool, which was invaluable throughout the study.

The relevancy criteria of literature evolved as the research process progressed. It became apparent that professional identity studies in traditional professions like medicine, psychology and teaching were useful in understanding the phenomena but did not address the challenges and nature of emerging professions like intelligence analysis. Most of the existing literature dealt with typical challenges faced by these traditional professions, which have legalised standards, procedures and certifications while enjoying the legitimacy of public service and recognition by the authorities, which is not the case with intelligence analysts.

The search strategy (Appendix A) was redirected to emerging or "new" professions to compare whether the construct, as manifested in the traditional professions, applies to intelligence analysis. This opened up new avenues in the literature, especially in organisational studies, where the study's international perspective linked with the literature on professionalism and identity management in global consulting or knowledge-intensive companies. In addition to the search strategy below, key authors and subject matter experts who served as references in original articles were identified and their work analysed to get a holistic picture of the different viewpoints on the dimensions this study address.

The richness and diversity of scholarship in the different fields are evident in the fact that only five "main authors" (those with more than three articles in the list of the relevant sources) in the security field, three in the field of sociology of professions, and six in the field of professional identity were identified. Those aspects of intelligence and intelligence analysis relevant to this study offered no "main" authors but about 80 individual authors, while the total of authors whose work was used in the literature review amount to 736 authors of whom at least a third co-authored. Of course, only those authors whose work are cited are included in the bibliography.

2.3 The security risk intelligence analysis context

2.3.1 Intelligence analysis in context

Although intelligence has a very long history dating back from Biblical times when Moses sent a reconnaissance team to Canaan and Sun Tzu wrote his seminal *The Art of War* in the 6th century B.C., there is no evidence that intelligence analysis as a separate role existed before the first analysts were appointed in 1942 in the US Office of Strategic Services (Duvenage, 2010). Previously, the intelligence operative or his client in the military or diplomatic service evaluated and interpreted the raw information themselves. Civilian government intelligence was only established at the height of World War II, and until recently, had the monopoly over intelligence functions. However, many other institutions, companies and other actors now "practice" intelligence, often to protect overlapping spheres of influence or interests—whether it is their own, the community in which they operate or broader national interests.

This radical "expansion" of intelligence (Petersen and Tjalve, 2018) has been forged since the early 2000s as a reaction to prevent and manage the myriad complex and unknown threats that did not discriminate between government targets and those of companies or the general public. The role and function of intelligence analysts are multi-pronged. In the first context, it is to provide the decision-maker with situational awareness. The analyst should provide context through description, explanation, and interpretation to understand developments that will then inform their judgements (Bielska & Pallaris, 2017). Secondly, analysts should provide foreknowledge by anticipating future developments and alerting stakeholders to the potential impacts. Intelligence analysis is uniquely geared to assist in this uncertainty management as it seeks to identify strong and weak signals that could be cues for future events and trends. Intelligence analysts, whether they serve in the government or private sector, and whether they analyse terrorists, criminals, foreign governments and armies, business competitors or pressure groups, share the same core professional function. The cognitive processes, knowledge dynamics and methodologies of knowledge creation and sharing are the same in both the government and private sector domains.

2.3.2 Security risk intelligence analysis in the private sector

This thesis focuses on those intelligence analysts who work for specialist political risk vendors and corporate security departments. It does *not* include private security and intelligence contractors who perform intelligence work for government agencies. Typically, the intelligence function will be situated in the corporate security department as the latter is responsible for identifying and effective mitigation and management of all events that could threaten the corporation's sustainability (Manojlovic, 2014). The security department is strategically linked to the corporate risk management system through its placement in the broader "operational risks" category of the organisation-wide risk management framework. When optimally utilised, the security risk intelligence function serves as an early warning system (Pate-Cornell, 2015) that detect signals of emergent threats and feeds them into the risk management system where the risks are appropriately analysed, weighed and managed according to the corporation's risk assessment methodology and risk appetite. Dvojmoč (2019) stated that security risk intelligence is an "unavoidable and necessary tool" for a company's risk management and its objectives to achieve competitiveness and security in its global business.

In practice, the security intelligence analysis function will execute the main activities of monitoring, assessing, analysing, reporting and liaising with different stakeholders on any or all of the following areas:

- Political stability and security situations of areas or countries where the company has interests or employees;
- Travel risk security that could require additional protective protocols for employees and executives;
- Profiling of persons or groups of interest that might pose a threat to company employees, executives, Board members, facilities and processes;
- Due diligence and background checks on possible insider threats, potential employees, major suppliers or contractors, mergers and acquisitions;
- Investigations or investigation support of criminal or security incidents in the company;
- Reputational risk and negative media monitoring;

- Crime patterns and activity analysis around company premises to determine risk in terms of duty of care responsibilities;
- Corporate espionage and sabotage activities by competitors or nation-state actors;
- Detection and prevention of cyber intrusions and attacks against the company
- Intellectual property right infringements and crimes
- Supply chain resilience
- Insider threats and integrity management

For purposes of this study, the term SRIA will encompass those with job titles of security risk or threat analyst, crime analyst, crime intelligence analyst, research specialist, political risk analyst, cyber threat analyst and the like, who all share the above mandate and work in the private sector.

2.3.3 An emerging profession

Security risk intelligence analysis is regarded as one of the new, knowledge-based occupations that appeared to have side-stepped the traditionalist professional model due to changes in society that required the private sector to have a similar threat intelligence function than governments had. Consequently, this study classifies it as a profession as the criteria have been relaxed to insist that the occupation is mostly skills-based and often education-based. “Profession” is often used as an adjective rather than a noun (Ibarra, 1999). Being a professional now describes how individuals carry out their work with knowledge and skill rather than the specific kind of work they do.

Furthermore, as an emerging profession, intelligence analysis has no strict rules, standards, legal governance structure, mandatory professional membership, official credentials, and an established body of knowledge and does not necessarily serve the public good as traditional professions like medicine and law. Furthermore, intelligence analysts are also part of the “knowledge worker” cadre that now constitute about half of the world’s workforce (Brown, 2019). Knowledge workers are usually highly qualified, and their work is characterised by creativity, problem-solving, networking and task

complexity while they espouse specific, rare and abstruse knowledge that they apply in the work context (Costas & Kärreman, 2016).

Despite rigorous research on analytical methods and techniques, there has been no research on intelligence analysts' professional identity in either the government or private sectors. In the only ethnological study into the lived experience of intelligence analysts in the CIA, Johnston (2005) commented on how analysts in the CIA would explain what it is they do. By extension, they believed this who they are. However, social psychology provides valuable theories to put a study on security risk intelligence analysts' professional identity on a solid foundation that can serve as the basis for further research. The main reason why the focus is only on these professionals in the private sector is that access to intelligence analysts in the government and law enforcement environment would have been nearly impossible to achieve.

2.4 The Professional Identity construct

2.4.1 Social psychology theories underpinning the professional identity construct

Individuals' professional identity is rooted in their psychological make-up, specifically their individual and social identities within a work context. The identity construct has been studied since people asked the question "Who am I?" and explained the individual dimension of identity by referencing personal attributes like values, characteristics, roles, ideas and their interpretation of experiences.

Also, the individual lives in a social context that impacts his identity—the identity is socially constructed. The social psychology discipline traces the roots of identity theory to GH Mead, who asserted in the 1930's that "society shapes self, shapes social behaviour" (Stryker & Burke, 2000). This societal aspect means that the personal identity is socially constructed and informed by one's relations with others – what they think of one, what one thinks of them, how one thinks of oneself and what one thinks others think one is. Inevitably, the understanding of a person's concept of self culminates into multiple personal identities that interpret the interaction with other individuals or groups and chooses which identity to "activate" depending on various factors, including

salience and status—the social dimension of identity (Cardoso, Batista, & Graça, 2014). Booysen (2018) explains the complexities of identity, defining it as

> "multifaceted and multiple, consisting of fixed, fluid, shifting and temporary; independent and interdependent, enhancing and conflicting; complimentary and contradictory identities, differing in prominence and salience based on contextual fluctuations and regulation. Many of our actions are driven by the struggle to defend, maintain, enhance and produce congruence in our identities."

Four inter-related and sometimes overlapping social psychology theories or conceptual frameworks, namely role identity theory (RIT), social identity theory (SIT), self-categorisation theory (SCT) and the collective identity theory (CIT), offer insights into the dimensions of the Professional Identity construct used in this study. While interacting with the social environment, the individual reconstructs his identity by adopting roles (RIT) that enable him to manage situations within the social context and rationally categorise or align himself (SCT) with or separate from a specific group in a specific context (SIT). The Collective Identity theory further places the individual where he shares the same sense of belonging with others. The following section provides a brief interpretation of the four theories as they relate to this study.

i) Role identity theory (RIT)

People play different roles in life, often simultaneously. The Role Identity theory (RIT) asserts that identities are internalised role expectations (Stryker & Burke, 2000) attached to positions occupied in networks of relationships. RIT focuses on the individual's need to manage the diversity among the multiple roles (and corresponding expectations) that an individual holds (Roberts & Creary, 2013).

The prominence or prioritisation of a role identity depends on whether one gets support from others for that identity, the extent to which one is committed to that identity and whether one receives rewards from that role identity (Stets & Burke, 2000). The greater the commitment and salience to a particular identity, the more likely the individual will be motivated to bring his self-concept in line with the role expected of him. Contrary, when the individual is not committed to a role identity or have problems verifying his role identity due to a lack of or negative social structure feedback, the individual will

extract him from that social structure, often leading to the disintegration of the social structure (Stets & Burke, 2003).

For purposes of this study, it is assumed that the role identity of a security risk intelligence analyst is but one of the many role identities that a person would have, albeit perhaps the main work-related role. The prominence of the identity amongst the analyst's other roles would depend on whether the role is supported or accepted by others (including the organisation, co-workers and personal social structures, the analyst's commitment to (or passion for) the role and the physical or emotional rewards the role offers. The conventional dimension of the security risk intelligence analyst's role expectation would be found in the organisational job description or the role profile, including the tasks and responsibilities, minimum qualifications, experience, and skills the person fulfilling the role is expected to have. Each organisation's social structure would have different role expectations depending on the nature, purpose and roles within the organisation—the analyst for a pharmaceutical company might have a different job description or title than the one working for a private security consultancy, although the role outcomes of all SRIA would ideally be more or less similar (see Appendix B for job advertisements). The idiosyncratic dimension of the analyst' professional role identity would be those personal traits, expertise and experience each analyst would bring to the role. The latter then also explains the difference in role execution of people who have the same job description/role in an organisation.

There has not been much research on how people define new roles in the absence of "conventional" expectations, especially in the postmodernist age, where the world of work is changing dramatically. Like security risk intelligence analysis, new professions are continuously emerging while some traditional vocations have become extinct (Bersin, 2017). To a large extent, emerging professions "build the plane while flying" as they might only have a broad sense of what roles they could play in an organisation, and are therefore filling gaps as they emerge, or creating new opportunities that open up as the world of work evolves.

ii) Social identity theory (SIT)

Social identity theory (SIT) defines an individual identity as 'that part of the individual's self-concept which derives from his knowledge of his membership of a social group together with the value and emotional significance attached to that membership' (Tajfel, Billig, Bundy, & Flament, 1971). The two leading proponents of the SIT, Tajfel and Turner (2004), propose that individuals look for a positive sense of self and compare their group with other groups based on various categories and tend to create a favourable distinction for their group—who we are and who we are not. Tajfel and Turner's work focused mostly on stereotyping and discrimination in the sociology field. Group categories that people belong to can include company, occupation, gender, nationality, ethnicity and age (Ashforth & Mael, 1989), amongst others.

SIT examines how people understand and position themselves and others in terms of social group categories (i.e. in-group/out-group) and how one's identity stems from the adherence and membership to social groups, such as organisational- and occupational sub-collectives (Aangenendt, 2015). Social identity and group membership is thus part of a person's sense of "'who they are" (Haslam, 2004) and fulfil the individual's needs for self-enhancement, belongingness and differentiation (Roberts & Creary, 2013). Identification with a group is a psychological process and requires no social interaction with others in the group (Ashforth & Mael, 1989; Brooks, Riemenschneider, Hardgrave, & O'Leary-Kelly, 2011), implying that identification can even arise in the absence of interpersonal relations, similarity or interaction and still have a powerful impact on emotions and behaviour of the individual.

Professional identity is one of the multiple social identities an individual holds, and the SIT theory deduces that people can feel themselves part of, and behave as part of this professional identity, whether they have actual contact with the social group or not. In organisational terms, social identification enables the individual to associate himself and feel loyal (or disloyal) to an organisation or corporate culture (Ashforth & Mael, 1989), or in this study's case, a profession/occupation such as security risk intelligence analysis. The process through which this happens is found in Turner's related self-categorisation theory.

iii) Self-categorisation or self-identification theory

Self-identification theory (SIT) or related self-categorisation theory (SCT) aims to "understand, explain and predict how people come to think, feel and act as a psychological group and, importantly, the circumstances when this will occur and its consequences" (Turner & Reynolds, 2012). The act or process of self-identification is first and foremost cognitive where one is aware of membership, evaluative where one makes value connotations to that membership and affective, where one invests emotionally in that awareness and evaluation of membership (Tajfel, 1982).

Ashforth, Harrison and Corley's (2008) continuum of identification (Figure 1) explains that the cognitive and affective aspects of identification are the core attributes of identification where the person defines himself as something or someone because it is important to him and he feels good about it. As the formulation of identity broadens, the content of the identity, or the enduring attributes that constitute identities—in this study, what it means to be "A" or a security risk intelligence analyst—is revealed. These attributes include values, goals, beliefs, traits and knowledge, skills and abilities. The dotted ring between the core and the identity content depicts the fact that identities do not necessarily include all of the content attributes because they might be emergent,

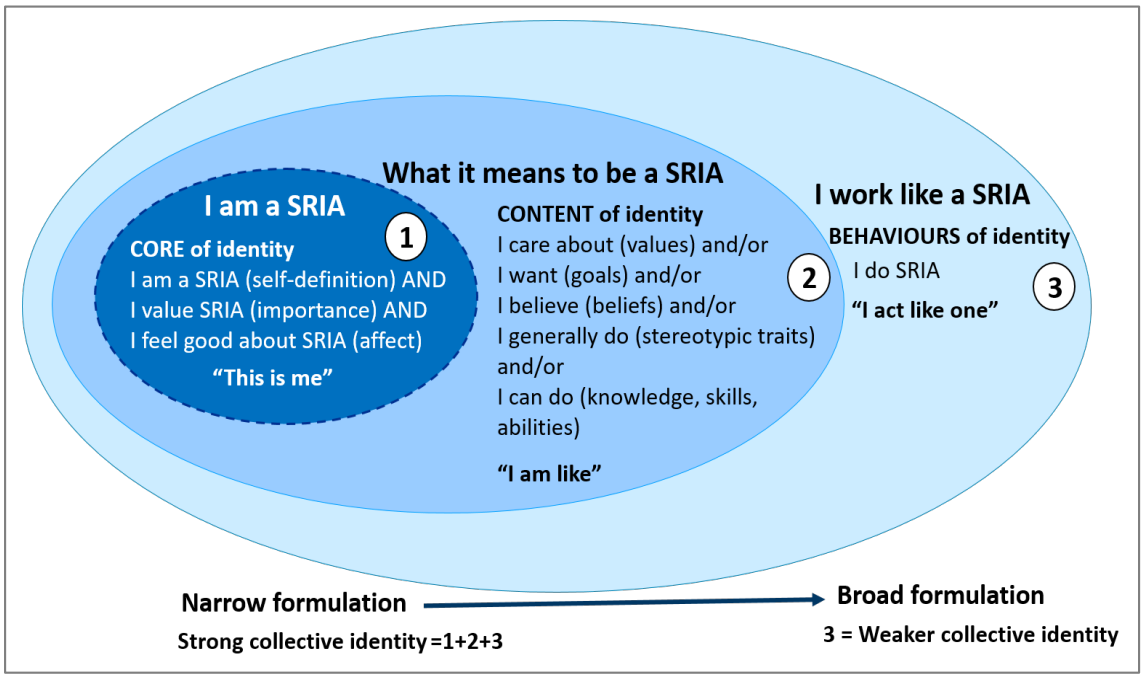


Figure 1: Continuum of professional Identification of the Security Risk Intelligence Analyst: based on Ashforth, Harrison and Corley (2008)

unclear or tacit when identifying with a role or collective; one would not necessarily accept some of the content attributes. Behaviour related to the identity is the furthest from the core of identity, depicting that behaviour is a probabilistic outcome of identification and not a necessary component. Although behaviour is supportive of the identity most of the time, situational constraints might weaken the link with the core and content of the identity. In this study's context, a person might self-identify as a security risk intelligence analyst in the sense that he might value the importance of the role and feel good about the impact he has on a company, but he does not necessarily espouse some values or does not necessarily have the competency to do certain types of analytical techniques associated with the role. Furthermore, a manager who insists on 'doctoring intelligence' to suit a client's expectations might induce the analyst to omit certain information, thereby acting against her ethical principles.

Identification or categorisation is the fundamental basis of our social interaction with other people, with psychological and demographic variables (Haslam, 2004) playing a decisive role in seeing ourselves vis-a-vis others. Most problems in society and organisations stem from the friction of fault lines between how we perceive ourselves against others and with whom we self-categorise depending on our interests or priorities. One first has to place oneself or categorise oneself, either deliberately or unconsciously, in terms of a specific grouping before one can feel proud to be a member of the social group. One would execute the process of self-categorisation based on an array of social stimuli, which one sorts into a basic level of categories based on the similarity or dissimilarity and then puts oneself into the most similar category (Ashmore, Deaux, & McLaughlin-Volpe, 2004).

The basis of the categorisation depends on the individual's perception of certain properties of the stimuli, the situation and the different goals and motives of the individual in the situation. Self-categorisation is also a dynamic process as the individual defines himself in different ways in different situations (Turner & Reynolds, 2012) depending on how he makes sense of the stimuli. Therefore, self-categorisation is flexible and can change because of the dynamic interaction between the self, context, and others.

People could be hesitant to self-categorise where group boundaries are ambiguous and porous. They might feel they are not fitting the prototype group members, or consider themselves marginal group members or that their membership will not be regarded positively (Ashmore et al., 2004). Self-categorisation also implies that when an individual identifies with and conforms to norms associated with the social group, his idiosyncratic views become socially organised and consensual. In this process, individual views are coordinated and transformed into the group's shared values, beliefs and behaviour (Haslam, 2004). Turner and Reynolds (2012) assert that self-categorisation and social comparison affect personal identity and that social identity processes can even impact cognitive performance, personality, and well-being.

SCT is a useful theory for this study as it explains the analyst's willingness to identify with and self-categorise as a member of the security risk intelligence analyst social group. The socialisation of the personal viewpoints to become the group's viewpoint and normative behaviour also explains collective identity. As social groups' formation is dynamic and fluid, one might not even be aware of the existence or the emergence of a social group until one is confronted with a new situation, information or stimuli that opens up the opportunity to self-identify. In some instances, participants in this study only started to self-categorise as security risk intelligence analysts when the study was advertised with the requirements of participation set out the "typical" security risk intelligence analyst targeted for inclusion.

iii) Collective identity theory

Ashmore et al. (2004, p.81) incorporated all three previous theories in their collective identity constructs in which they define collective identity theory as "one that is shared with a group of others who have (or are believed to have) some characteristic(s) in common." The prerequisite here is self-categorisation of the individual—individuals in the social group must acknowledge their belongingness to that group before collective identity could emerge. Collective identity implies the individuals' belief in categorical membership and a set of cognitive beliefs associated with that collective, including stereotype traits, ideology, values, and emotional connotations. They specifically identified seven individual-level elements of collective identity:

1. Self-categorisation wherein the individual places himself in a social group due to his perceived similarity in one way or the other with the group;
2. Evaluation refers to the positive or negative attitude the individual will have towards the social group he identifies with;
3. The degree of importance of group membership to the individual's overall self-concept;
4. The affective sense of belonging or attachment and sense of interdependence with the social group;
5. The degree to which the individual is socially embedded with a particular collective identity;
6. The extent of behavioural involvement with the social group and
7. The content and meaning the collective identity provides to the individual in terms of how the individual associates self-descriptive characteristics with the group, the group's ideology and group narrative or history.

2.4.2 Defining Professional Identity

The world of work encompasses all levels of identities—individual identity, group identity, professional identity, interest group identity, hierarchical group identity and the organisational identity as well as the individuals' self-categorisation with all of these identities (Aangenendt, Kuijpers, & Sanders, 2012; Beech, Macintosh, & Mcinnes, 2008). This section provides an overview of the construct of professional identity, explaining what it is, why it is essential, and its different dimensions.

Most definitions of Professional Identity concur that there are two critical aspects to the professional identity construct: one intrapersonal or idiosyncratic and the other interpersonal or social (Caza & Creary, 2016; Cowin, Johnson, Wilson, & Borgese, 2013; Ibarra, 1999; Nuttman-Shwartz, 2017; Tsakissiris, 2015). The idiosyncratic dimension relates to the image the individual has of his attributes, values, motives, experiences, type of education, training, and skills to "do a job". The social dimension relates to a group of people, individually and collectively, sharing the same image or approach to a particular type of work.

For the purpose of this study, professional identity is defined as that social identity that is focused on an individual's sense of self about their occupation, work or professional life (Fraser-Arnott, 2019) that creates a psychological attachment between the individual and a particular profession consisting of other individuals sharing the same identity (Tsakissiris, 2015).

It is necessary to clarify another construct that will be used in this study—organisational identity—which implies the individual's perception of oneness with, or belongingness to, an organisation where he defines himself in terms of the organisation of which he is a member (Mael & Ashforth, 1992). As this study's main focus is on the individual's sense of belongingness to the profession, it only mentions organisational identity in a cursory manner when the participants explicitly link this sense of attachment to their employing organisation with their individual professional identity. Organisational identity should not be confused with organisational commitment or corporate identity, which refers to the branding and marketing of corporate images and reputations. Ashforth, Harrison and Corley (2008) stated that organisational identity is another way people define themselves and make sense of, and navigate their place in the world.

Identifying with an organisation also fulfils the need to associate with abstract, larger entities and the individual's need to enhance his interests in this larger association. As with professional identification, organisational identification rests on the premise that the individual can associate himself with the values that the organisation presents, leading to employee satisfaction, engagement and meaningful work. There is a definite correlation between organisational identity and other organisational behaviours, including leadership, perceptions of justice and corporate citizenship.

2.4.3 The elements of Professional Identity

The professional identity construct has four main elements or characteristics.

i) It is multifaceted

The first is that it is multifaceted, as an employee fulfils various roles for which they have different identities at any given time or situation, with different personal characteristics,

personality and character attached to that identity (Aangenendt, Neelen, Willemse, & Laven, 2018). Professional identity is a unique, complex construction of multiple identities with different strengths that the individual perceives himself in the context of his work.

ii) It is dynamic and ever-changing

Professional identities are also *dynamic and ever-changing*, especially in the complexity-driven world of work and social interaction in the post-modern age. Individuals' identities can adapt and develop over time and can become more or less important to the individual (Aangenendt et al., 2018) depending on personal motivation for self-categorisation (which includes self-enhancement, the need to feel a sense of belonging, self-affirmation etc.), life changes and conflicts with other identities that are negotiated continuously to maintain equilibrium. In the same way, professional identity is an ongoing internal process of interpretation and re-interpretation or sense-making of experiences (Beijaard, Meijer, & Verloop, 2004; Fraser-Arnott, 2017) or external factors like personal life changes, career phase, organisational interventions, developments like leadership support or the lack thereof and one's own professional development strategy (Aangenendt et al., 2018). Both the individual and the collective professional identity need to be able to adapt to the change in the environment to remain relevant.

iii) It has individual agency

Individuals are active authors of their identity scripts (Bévort & Suddaby, 2016) and affirm the self-categorisation theory that individuals actively and cognitively interpret and act to improve their self-image and self-efficacy in their work context. A person's professional identity is thus central to his sense of agency, developed through interactions at work and is therefore both a product and an agent of systems and structures in the workplace (Briggs, 2007).

iv) It is shared with others

Based on social identity theory, professional identity is the values, beliefs and practices held in common with others who work in similar environments or perform similar tasks. The interaction and identification with similar others impact one's identity throughout

one's career in a continuous feedback loop of socialisation, sense-making and experiences (Fraser-Arnott, 2019).

2.4.4 Antecedents to professional identity

In their research on the factors impacting the professional identification of IT professionals, Brooks et al. (2011) found that four factors impact a person's professional identity, namely 1) his need for professional identification, 2) the perceived similarity to others in the same profession, 3) the individual's perceptions of the profession and 4) the public's perception of the profession. The "need to identify" relates directly to role identity theory and self-categorisation theory, where the individual attached himself to a group based on his personal needs or motivations. The "similarity" construct reinforces the sense of sharing similar beliefs, attitudes or purpose discussed above in the relevant theories–the higher the sense of similarity, the higher work satisfaction and positive evaluation of the profession. In their research, the "personal perception" of the profession, both when initial contact was made with the profession and during their career, was the strongest construct impacting an individual's professional identity. The fourth factor, public perception of a profession, only plays an indirect role in professional identification, which they found not to be determinant of the strength or the intensity of the individual's professional identity.

2.4.5 The value of understanding professional identity

In organisational studies, it has been found advantageous to study how professional identities are constructed, the interaction between the different identities and how it influences the effectiveness of individuals, groups and the organisation to deliver services and products to stakeholders, clients and the broader community. Through the construction and maintenance of a professional identity, individuals derive meaning and purpose for themselves in serving and contributing to society, while a strong professional identity is associated with more satisfied employees and higher quality of work (Caza & Creary, 2016). The internalisation of professional roles, norms and values also impact employees' attitude towards work, and ultimately their self-esteem and psychological well-being (Alvesson, 2011).

A strong collective professional identity contributes to a shared frame of reference, better communication among the professionals, optimal multidisciplinary collaboration and more efficient organisational outcomes (Molleman & Rink, 2015). On the other hand, when employees lack a collective professional identity, they will struggle to convince society of their value and legitimacy (Thomas, 2016).

The literature on 'professional identity' covers diverse fields, including counselling and clinical psychology (Alves & Gazzola, 2011; Burns & Cruikshanks, 2017; Fisher, 2017; Mellin, Hunt, & Nichols, 2011), social work (Weiss-Gal & Welbourne, 2008), education (Brott & Myers, 1999; Cranitch, 2017; Rewolinski, 2014), the broader medical professions (Brandis, Fitzgerald, Mcphail, & Fisher, 2016; Elvey, Hassell, & Hall, 2013; Kumpusalo et al., 1994; Molleman & Rink, 2013), journalism (Aldridge & Evetts, 2003; Ferrucci & Vos, 2017; Grubenmann & Meckel, 2014; Li & Chitty, 2017), information technology (Brooks et al., 2011; Smith, 2016) and library and information sciences (Fraser-Arnott, 2017; Goertzen, 2018; Hicks, 2016). In recent years, newer professions' identity has been studied, including that of personal coaches (Gray, Saunders, Curnow, & Farrant, 2015), sign language interpreters (Harwood, 2017), evaluators (Ball, Biesheuvel, Hamilton-Baillie, & Olonisakin, 2007; Jacob & Boisvert, 2010; Levin-Rozalis & Shochot-Reich, 2009), women engineers (Plett, Hawkinson, Vanantwerp, Wilson, & Bruxvoort, 2011), archaeologists (Shaeffer, 2016), women military interrogators (Dorough-Lewis, 2017) and even massage therapists (Sullivan, 2012) and chefs (Rehn, 2012).

2.4.6 Stages of Professional Identity construction

Professional identity formation is an ongoing process throughout one's life and is most often a complex, individualised process that cannot be prescriptive or generalised. However, Jebril (2008) identified four broad stages of professional identity development that help researchers understand the phases an individual experience in his quest for professional fulfilment (Figure 2).

In the first stage (the *preoccupation stage*), a child is exposed to different professions through social interaction with family, school, friends and the media. It is in this stage

that core values, personal characteristics, strengths and weaknesses are formed. In puberty, the adolescent will start searching for a profession that matches his personality, values and strengths. The level of self-knowledge and exposure to career options will impact when and whether the young adult can move to the next stage or continue to search for the appropriate career fit.

The next stage, the *learning stage*, lasts from formal education until the first formal employment and is the most intensive stage in professional identity construction. During this stage, the individual learns the profession's theoretical underpinnings, gain knowledge and skills, and learn the professional language, ethics, and morals. The individual will also socialise with others in the same profession, thereby affirming that the chosen career fits his values and professional self.

The third stage, the *professional stage*, lasts from first employment until retirement. In this stage, the individual closes the gaps between theory and practice, continuously learns or develops new professional related skills, strengthens socialisation with peers, specialises or diverts into the management stream and even mentors new professionals. This thesis mainly deals with this stage of professional identity development, the *professional stage*. In the last stage, the *post-professional stage*, people can choose to forego their previous professional identity altogether by either starting a new career or mentally and physical retiring from all semblance of professional activity. Others might choose to invest in the profession by becoming mentors or teaching at universities and private training companies.

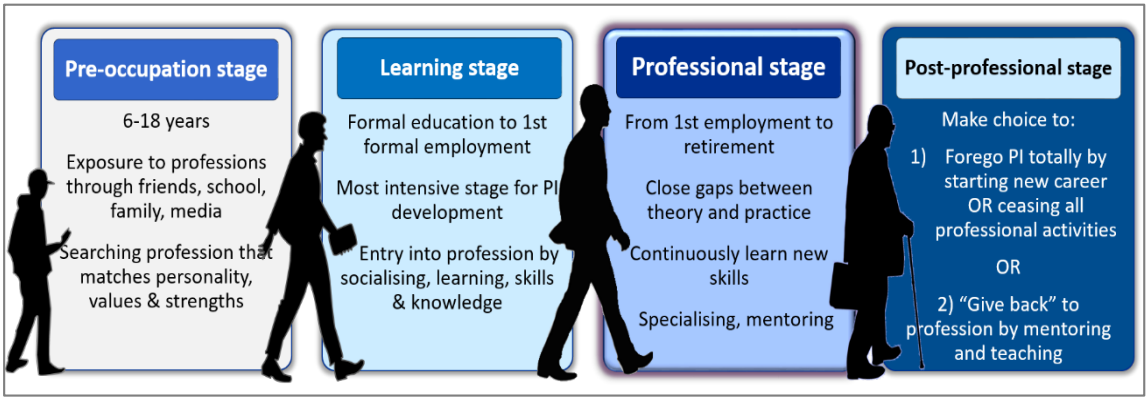


Figure 2: The four stages of professional identity construction, based on Jebril (2008)

2.4.7 Typical professional identity struggles and their coping mechanisms

During the professional stage, the individual will often experience identity crises or struggles that would require her to execute coping mechanisms or strategies. The literature on the types and nature of professional identity tensions people experience is very limited. The literature defines the continuous process of juggling and renegotiating professional identity due to changes in the individual's own expectations, new organisational practices, structures and roles, and societal complexities on professional identity as *identity work*. It includes the "cognitive, discursive, physical, and behavioural activities that individuals undertake intending to form, repair, maintaining, strengthening, revising, or rejecting collective, role, and personal self-meanings within the boundaries of their social contexts" (Caza, Vough, & Puranik, 2018). Identity work has a dual nature: inward-looking, where an individual actively constructs his professional identity through his sense-making processes, and outward-looking, where the person interacts with and receive feedback from others. Identity work strategies can be grouped into two categories: identity protection and identity restructuring strategies.

i) Identity protection strategies

Individuals can *distance* or disassociate themselves from a social group and its negative stereotypes, as evidenced by Cobbold (2015), who concluded that Ghanaian teachers dissociate themselves from the professional teaching body but still see themselves as professional teachers. More often, one would engage in *impression or image management* when there is an effort to restore a group's positive distinctiveness by dispelling negative stereotyping. Individuals working in occupations that are often stigmatised or considered "dirty", like coal workers, garbage collectors or socially "unacceptable", like massage therapists, would recalibrate and reframe their identities by internally enhancing the positive aspects of the profession (Butler, Chillas, & Muhr, 2009; Kreiner & Ashforth, 2004). Externally directed image management strategies would include awareness campaigns, change in appearances (like changing uniforms), rhetoric and public relations drives (Alvesson, 2001; Brouard, Bujaki, Durocher, & Neilson, 2017; Roberts & Creary, 2013).

ii) Identity restructuring strategies

Identity restructuring responses usually occur when the professional identity is challenged in social interaction with new networks, new role expectations, when there is self-doubt in complex or problematic social institutions or when there is a mismatch between self-understanding and the social role expectations (Alvesson, Ashcraft, & Thomas, 2008). An individual would restructure his identity if it is advantageous to him or leads to self-enhancement by associating with perceived prestigious collectives, enhancing his distinctiveness from others, and the need to belong or feel connected to others (Caza et al., 2018). Individuals would also apply different strategies simultaneously, which sometimes lead to further identity conflict until they succeed in executing the most appropriate strategy within that specific context. Identity work restructuring strategies among surgeons (Pratt, Rockmann, & Kaufmann, 2006) include enriching (where one's understanding of what their profession means to them and society is deepened), patching (when one use elements of another "better" identity to reduce deficiencies in the current identity) or splinting (when one adopts a previous stronger identity to strengthen a current weaker one).

Kreiner, Hoolensbe & Sheep (2006) identified different categories of identity work in their research among Episcopal priests relevant to other professions. The first identity work category is segmentation or compartmentalisation tactics, where individuals who perceive too much identity tension in favour of the collective professional identity will employ tactics where their personal identity balances out the demands of the collective. These coping mechanisms include setting limits to execute a role, creating an identity hierarchy, escaping into a totally different role or deciding when to activate or deactivate specific identities to suit a particular context. The second category, integration or blending tactics, is useful in understanding how individuals manage multiple professional identities or where there is not sufficient professional identification on an individual level. Here one merges one's role (what one does) with one's identity (who one is). Individuals could either fully integrate themselves or only some aspects of the self with the profession or even go so far as to see themselves as embodiments or symbols of a particular identity.

In summary, professional identity management is dynamic and dependent on the individual's contextual interpretation of self-interest in the midst of competing for social demands and personal self-interest. In all cases, each individual's self-awareness of his role as a professional would determine the extent to which identity work takes place and the extent to which he associates with collaborative professional identity endeavours. Every person will have their own complex set and degree of self-awareness and self-interest, and it would be difficult to theorise generally due to these factors.

2.5 Collective professional identity

Fundamentally, the professional identity construct is dualistic; it is simultaneously individual and collective due to the social interaction between the employee and the professional group he considers himself to be a member. The study of collective identity has different schools of thought: for psychologists like Ashmore et al. (2004), collective identity is a psychological concept that refers to the individual's belief that he is a member of a specific group because of shared values, cognitive qualities, stereotypic traits, ideology or objectives, and not the group's collective feeling of being the same in some sense. In contrast, organisational studies and sociology scholars like Alves & Gazzola (2013) and Evetts (2011) argue that to disregard the contribution of the collective group's sense of commonalities and only focus on the individual sense of belonging does not acknowledge the complexity of professional identity.

In this thesis, the two viewpoints are merged to study the collective identity of the professional group, SRIA, first to determine if individual analysts self-categorise as being members of the group and secondly, what the perceived elements and strength of the shared membership, beliefs, traits and values of the collective group are. Thus, collective professional identity is defined here *as both the individual's sense of belonging to a professional group and the group's shared behaviour and values, perception or collective action.*

Until recently, identity researchers such as Groth (2015) used Ashmore et al.'s (2004) collective identity construct based on individual self-categorisation theory to explain collective professional identity. However, Bayerl et al. (2018) asserted that the Ashmore

construct was not appropriate for professional identity studies as the individual-level elements could not fully accommodate professions' peculiarities, such as specialist knowledge or roles or occupations across national contexts.

This limited the conceptual understanding of how the collective understand and describe themselves collectively–what Bayerl et al. (2018) call the "collective framing of professional groups". This gap limits our understanding of how professional collectives perceive themselves and how differences between different professional groups and even disconnects or dis-identification between the individual and the professional collective impact several professional related aspects such as career choice, commitment or job satisfaction.

Bayerl et al. (2018) were the first to identify professional identity self-descriptions from diverse professional groups across different countries. They used police officers and market researchers from four nationalities to answer "What do you associate with being a police officer/market researcher?" in a 20-statement test analysed with content analysis methodology. They identified five themes that frame how people collectively make sense of their profession, namely people (who we are), work (what we do), environment (where we are located), valence (what we get out of it), and profession (what our profession is like) as seen in Figure 3. Their research showed that these five themes remained constant across different professions and nationalities, although the emphasis or relevance on themes or topics may vary when people self-describe.

The identified "people" theme deals with people's description or perception of their personalities and how it fits their profession, what they can do in their professions, their attitudes towards their profession, the shared values and norms, and if and how they share a physical appearance.

The "work" theme comprises the description of the work members of the profession perform. They found that the members of a profession would have three *foci* of role descriptions: inward-directed (roles within the professional group such as "team member"), outward-directed (roles performed for stakeholders outside the profession such as "community advocate") and task-descriptive roles which focused on activities

and products such as "product developer". Furthermore, the topics they deal with while working and the products they deliver or results have pointed to the importance of professions' technical artefacts and practical accomplishments (Reed, 1996) to help define who they are.

The "environment" theme deals with the organisational and social environment in which the target group functions and the resources they need to fulfil their roles. Here, the specific type of knowledge needed to perform and the networks of stakeholders, both within and external to the organisation, are relevant. The "valence" theme describes the value of the profession to its members, including what they "get out" of being a member of a profession and how other people see them (the profession's image). Here,

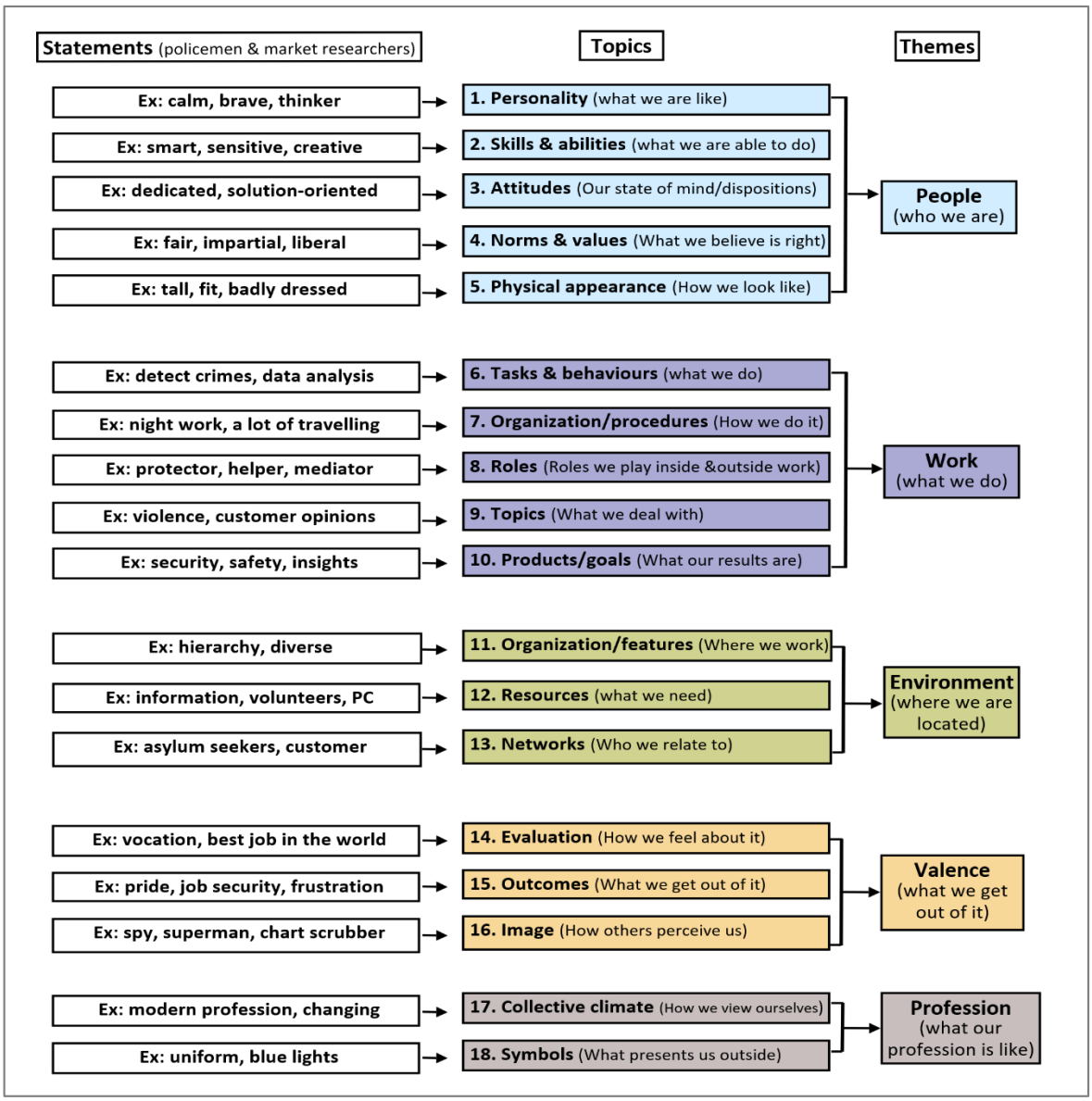


Figure 3: Bayerl et al (2018) Collective professional identity themes and topics in self-descriptions

statements dealing with evaluations of the professions, benefits and challenges represent the ability to be self-aware and critical of the external perceptions and how it might impact the profession's legitimacy in networks and society in general. Likewise, the "profession" theme describes the statements people make on how they perceive their collective profession in terms of changes, developments, trends and outward signs or symbols, which can be self-critical.

Some professions might not assign the same importance to symbols like police officers with their uniforms but might still have symbolic artefacts like "grey suits" for the market researchers that help them claim professional identity. In their research, Bayerl et al. (2018) discovered that market researchers' self-description was much more prevalent in terms of technical artefacts (their deliverables in the "work" theme) than symbolic artefacts in the "professional" theme.

This thesis supports the multi-dimensionality of the collective professional identity, being both personal and collective, and will use Bayerl et al.'s (2018) framework to investigate SRIA's collective professional identity in the private sector in Chapter 4. The absence of, or a weak collective professional identity, could affect both the individual and the group of professionals that feel they belong to the group. On an individual level, the professional would lack confidence in his skills and role in society. On a collective level, if there is a weak cohesiveness or a limited shared identity, the group will not have professional pride or would have difficulty in exerting legitimacy in society.

They will also not be able to communicate the specialist knowledge and value they bring to society as there is no shared frame of reference, which could enhance communication and collaboration internally and with external stakeholders. If a professional group or collective is not defined by its members, it may be mislabelled, misrepresented and wrongly defined by others (Alves & Gazzola, 2013).

Interestingly, an individual's personal identity and self-categorisation might be strong, while a social group's collective identity might be uncertain or vice-versa (Alves & Gazzola, 2013; Cobbold, 2015). A strong collective identity could lead to collective and collaborative practices and actions or not, depending on the purpose and ideology of

such a social group at a specific moment in time and context. This dynamism is acknowledged in this study as one of the unknowns in social group identity. When the collective professional identity is threatened or challenged by new technological advances like equity traders who have to compete against algorithmic internet "advisors" (Byrnes, 2017), or where a professional group, like accountants, experience large scale reputational damage, the professional group will employ identity work strategies, much the same as individuals would.

Typical responses to identity threats would include devaluating or derogating the threat, self-correcting or even socialising its perceived value through identity management efforts that would include new standards or ethical codes, or enhanced public relations to demonstrate the exclusivity, public benefit, or achievements of the group. Professional identity's complexity becomes more evident when professional organisations attempt to formalise collective professional identity across cultural and national borders. They often fail to implement global professional or education standards as it is seen as too prescriptive and ignorant of national or cultural contexts, in addition to prohibitive high membership fees. Often, these organisations reinforce the perception that Western or Northern Hemisphere countries impose "international" professional standards to maintain the uneven hierarchical power relations in the world without taking other cultures' work practices and traditions into account (Nuttman-Shwartz, 2017).

Whereas membership to these elitist professional organisations is often regarded as a testimony of competence and commitment in Western countries, it does not hold the same value and may be seen as irrelevant in developing or under-developed countries. Membership could become an impediment to professionals seen as "sell-outs" to Western dogma and expansionism. Regardless, there are still some professionals in developing countries who regard the membership of international professional organisations more advantageous for them personally than the perceived local antagonism against these organisations.

2.6 Conclusion

This chapter attempted to provide a concise representation of the existing literature related to the study. Although the study of professional identity, which originated in social psychology, has been a topic of interest in many disciplines, this study has identified the gap in security risk management and the nexus with intelligence analysis. The outcome of the literature review highlighted the various dimensions of individual and collective professional identity and the possible contributions this study can make to exploring and understanding the work-life of security risk intelligence analysts in the private sector.

Chapter 3

Methodology

3.1 Introduction

The purpose of this research study was to explore SRIA in the private sector's perceptions of their professional identity. An exploratory research approach is followed when the study's subject is relatively new, as is the case with this study. The researcher would then aim to find approximate answers to research questions that would satisfy her curiosity and desire for better understanding but not necessarily provide an accurate picture of the phenomena. Babbie (2015) also stated that an exploratory study tests the feasibility of a more extensive study of the topic and develop methods to be used in this subsequent study. Therefore, the study will also aim to examine which theories, concepts, and methodologies are appropriate for the subject matter.

In this study, the researcher believed that a better understanding of this professional phenomenon would allow analysts, their management, human resources personnel and learning and development specialists to maximise their impact on the organisations they work for and the broader society. On an individual level, the study aimed to understand the analysts' overall search for professional meaningfulness, job satisfaction, individual professional behaviour, functional duties, professional development, and their relationship with colleagues and clients. In seeking to understand the phenomenon across organisational and national boundaries, the study aimed to include participants from as wide as possible organisational and national contexts in the sample size.

This chapter outlines the research methodology used in the research study and explains how the pragmatist approach underpins the rationale for adopting a mixed-method design. A detailed discussion of each collection and data analysis method will be addressed separately in the following chapters dealing with the two separate studies' research instruments.

3.2 The research questions

This thesis aims to contribute to the understanding of the intelligence analysis profession by focusing on the collective and individual professional identity of practitioners in this field. The research objective was first and foremost to determine whether there is an emerging profession in the security risk intelligence discipline for analysts on an international level.

If such a profession did indeed exist, the second research objective was to explore the individual professional identity of SRIA in the private sector. Research questions on this level included the following:

1. How do they conceptualise their professional identity?
2. What is the perceived unique contribution of intelligence analysis in the private security sector?
3. How do intelligence analysts believe others perceive them?
4. What do intelligence analysts perceive as the opportunities and challenges inherent with their profession?
5. What experiences and conditions do intelligence analysts perceive as contributing to or strengthening their professional identities?
6. Is there a difference in the individual professional identity of analysts from different countries?

The third objective was to determine whether there is a collective identity of SRIA in the private sector on an international level, with the research questions related to this, namely:

1. Is there a shared professional identity across nationalities?
2. Is there a shared professional identity across organisational forms?
3. Is there a shared ideology and values of the profession?

3.3 The pragmatist research approach

Pragmatism is a relative newcomer to the research paradigm taxonomy (Tashakkori & Teddlie, 1998) and has grown in support amongst researchers who conduct mixed

methods research. Pragmatism does not take sides in the endless paradigm wars on the nature of reality or truth. Instead, pragmatism acts as a new paradigm that treats dichotomous classical research approaches as social contexts for inquiry as a form of social action, rather than abstract philosophical systems embodied in ontologies, epistemologies and methodologies.

Pragmatists argue that the aim of research should not be an attempt to most accurately represent reality but rather aim to be useful (Feilzer, 2010) to guide behaviour and lead to action. Pragmatism epistemology argues that knowledge is socially constructed through individual and shared experiences (Morgan, 2014) and that knowledge can only be acquired through the combination of action and reflection on the consequences of those actions (Biesta, 2010). For the pragmatist, knowledge should give practical meaning and action or problem-solving options in specific contexts; otherwise, it has no meaning or purpose. A pragmatic researcher embraces the ontological perspective (the nature of reality) of the social world as complex and reflects the flux of ideas, processes, experiences and practices of individuals and social groups.

Pragmatism as a philosophy reflects what Dewey explained when he stated that phenomena have different elements or layers, some objective, some subjective, some a mixture of the two. At the same time, there are layers of the "stable and the precarious" and layers of "completeness, order, recurrences which makes possible prediction and control, and singularities, ambiguities, uncertain possibilities and processes going on to consequences as yet indeterminate" (Dewey, 1925 cited by Feilzer, 2010) of actions and their consequences are contextual. Therefore there is no universal "truth" because people, situations and the consequences of their actions change continuously. The pragmatic research paradigm offered an epistemological justification and logic for using mixed methods (Johnson, Onwuegbuzie, & Turner, 2007) in the approach, instruments and analysis of the study of the professional identity of SRIA.

The one dimension of Morgan's interpretation of pragmatism that resonates in sociology, and specifically the first research question of this study (is there a shared professional identity among SRIA?), is the notion that beliefs or worldviews are socially

shared or interconnected although no two people have the same experiences or contexts in which they act. There are varying degrees of shared experience between people, which leads to different degrees of shared beliefs. In practice, this would mean that people might act in similar ways or give similar meanings to the contexts or consequences of their actions when they share beliefs about a particular situation, even if their contexts are socially or geographically different. The latter aspect strengthens the choice of pragmatism as an approach to study the professional identity of SRIA across organisational and national contexts.

3.4 Research design

The study's explorative nature dictated an inductive approach in which mixed methods was considered the most appropriate as the lack of literature on the topic gave latitude to the researcher to explore both the individual and collective professional identities to build the body of knowledge in this field. This research offers an innovative perspective on sociological literature (due to the target group) and the security and intelligence literature. It is the first such study on the topic and the target group.

The ultimate research objective—giving these professionals a voice to tell us who they are, what they do, what value they bring to the security sector and how they see their profession—endorsed the use of different instruments and analytical methods as it integrates both nomothetic and idiographic elements. Using mixed methods also enabled the researcher to draw from the strengths and minimise the weaknesses of the different methods (Johnson et al., 2007) and understand the nuances of this under-researched group's lived professional experience. This pragmatist approach revealed the different layers of intelligence analysts' professional identity by using quantitative methods to measure some aspects and qualitative methods to measure others (Feilzer, 2010).

Mixed methods research offered a framework for designing, collecting, analysing and interpreting data using both quantitative (QUAN) and qualitative (QUAL) methods within one or more of the research stages (Leech & Onwuegbuzie, 2009). The sequencing of mixed methods, the timing, weighting and the emphasis of one

instrument above another is an important factor in designing mixed methods research (Creswell, 2009; Leech & Onwuegbuzie, 2009). It was decided to approach the research as two distinct but interrelated studies in a sequential, equally weighted QUAN→QUAL approach where the quantitative study (Study 1), using a web survey, set the stage for the qualitative study, which used semi-structured interviews (Study 2).

This integrated sequential research design enabled triangulation as it provided the researcher with an understanding of the studied social phenomenon from different vantage points (Brannen, 2005). For this purpose, the research processes started with an integrated research design matrix which was developed to map the research objectives, the underlying theory or constructs, the possible questions for the two instruments, possible analysis dimensions and references to ensure that all nuances of the phenomena to be explored, were addressed and integrated into the two studies.

The aim of Study 1 was to provide contextual and descriptive data information on the collective professional identity of the target group and elicit participants for the interview study. The web survey questionnaire was designed to explore how the profession is perceived and constructed by those practising within the field by 1) exploring the employment and practice characteristics of intelligence analysts and 2) their perception of the role, contribution and future identity of the profession.

The quantitative study was mainly used as a fit-for-purpose approach to understanding the target group's geographic spread and demographics, coupled with their perspectives. The survey was piloted with four targeted participants from different countries to ensure that the questions were clear and unambiguous. Their feedback was positive, with a suggestion to add an additional question regarding the profession's future. A question, "In light of the fast-changing working environment, what skills do you think SRIA need to acquire to be relevant in the future?" was added.

The survey was only then launched by using various channels, including professional organisations, social media and email targeting. The survey was open for three months (1 November 2018 – 31 January 2019) on the JISC Online academic survey platform. The data was analysed using descriptive statistical analysis, nonparametric analysis and,

where applicable, with open-ended questions, thematic analysis with qualitative data. Chapter 4 will detail the methodology and processes used in Study 1.

Study 2, using semi-structured interviews as the data collection instrument, explored the individual professional identity of SRIA in the private sector. This study was designed to adhere to the principles and methodology of Interpretative Phenomenological Analysis (IPA). Interpretivism sees the world as too complex to be reduced to a set of observable laws (Gray, 2014), and therefore the interpretivist needs to get a richer and thicker understanding of reality as construed by social actors, specifically the differences between humans in their roles as social actors. Phenomenology sees social phenomena as socially constructed and is particularly concerned with generating meanings and gaining insights into those phenomena (Thornhill, Saunders & Lewis, 2009). Here, a specific type of question was formulated to extract detailed information of the personal lived experience, the meaning of experience to participants and how participants make sense of their experiences (Eatough & Smith, 2017).

The IPA method is idiographic and committed to understand phenomena from a first-person perspective, guided by phenomenological and hermeneutic enquiry. As can be seen from the flow diagram, the interviews (data collection) for Study 2 were held as soon as the web survey's data collection ended. The participants for Study 2 volunteered for the interviews in the survey and had to be approached before they decided otherwise or could not be reached. Interviews were held with ten participants, and the interviews were transcribed between 10 months and a year after the interviews. The results were analysed according to the IPA methodology and validated with the participants. Chapter 5 will detail the nature of IPA as well as the methodology used in Study 2.

The weighting of the instruments could only be judged after the completion of data collection as it was uncertain whether the web survey would have a high response rate and offer interviewee participants. The number and geographical spread of the survey respondents also had to reflect a sufficient sample size to be considered equal weight to the interviews. Fortunately, the sampling strategy was successful, and both

instruments and their results were equally important and integrated to reach the research objectives.

Finally, the findings from both instruments were integrated in Chapter 6 by exploring the similarities, differences and dimensionalities of the analysis to arrive at valid and well-substantiated conclusions about the collective and individual professional identity of SRIA in the private sector. The researcher found that the two instruments provided mostly confirming or complementary evidence and a few interesting contrarian viewpoints that gave a richer and deeper understanding of the different layers of the issue at hand. Figure 4 depicts the research design flow.

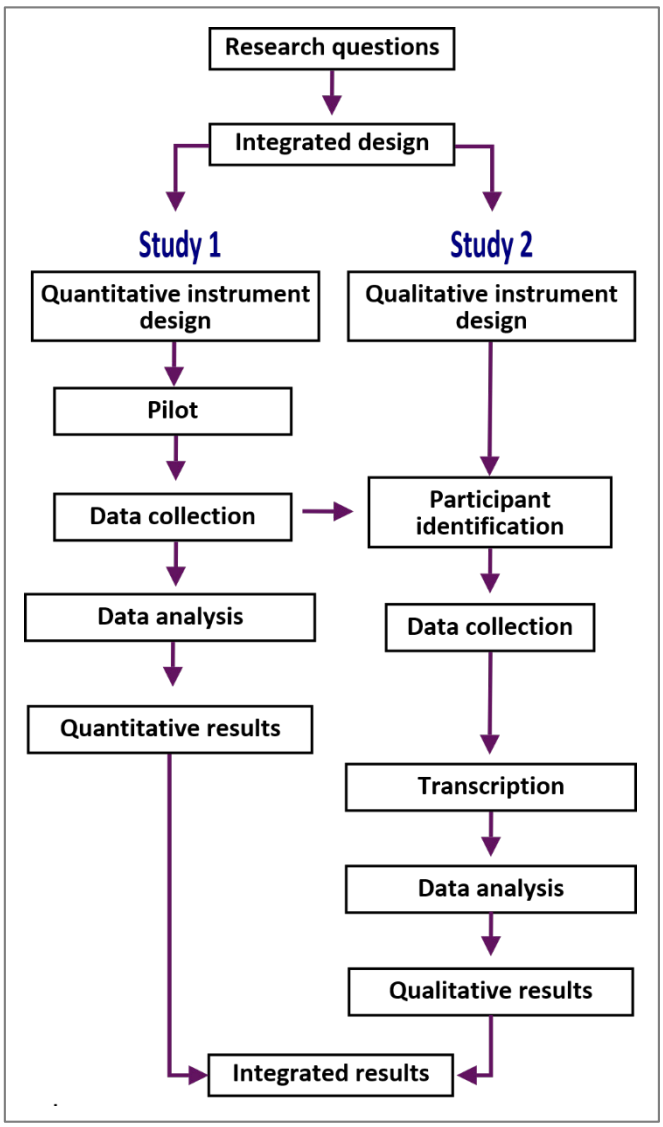


Figure 4: Flow of study's sequential mixed methodology

3.5 Sampling strategy

The sampling strategy was dictated by the research questions to determine an international perspective of the target group. The *sampling frame* for both research instruments (which will be dealt with in detail in the next chapters) was not geographically limited and comprised of those who *self-identify* themselves as a member of the security risk intelligence analyst profession—including those with the job titles of a security risk or threat analyst, crime analyst, crime intelligence analyst, research specialist, political risk analyst, cyber threat analyst, intelligence manager, security risk manager and the like. They were required to work currently in the private or non-governmental organisation (NGO) sector in any of the following:

- A private security company with its own security risk analysis capacity;
- A security/intelligence/risk unit in a company/multinational corporation whose core business is not security;
- A private company that provides security risk and threat intelligence consulting services to external clients, including the private sector or government agencies. This would therefore also include contractors who are embedded at government departments/agencies and private companies;
- A non-governmental organisation with its own security risk analysis capacity;
- An intergovernmental organisation with its own security risk analysis capacity;
- A researcher in the academia/institutions/foundations/think tanks whose primary function is to provide security risk analysis and advice to external clients.

Information on their functional responsibilities was obtained by integrating various vacancy announcements on the websites of companies and professional bodies like the Association for Risk Intelligence Professionals (AIRIP) and professional sites like LinkedIn (Appendix B). For purposes of this study, the analysts were required to either manage or conduct the analysis and interpretation of the possible impact of external and internal threats on the company or their client/s, including:

- Monitoring geo-political and socio-economic developments in countries where their company/clients have interests, including conducting travel risk analysis services to personnel;
- Analysing and advising on the prevention of cyberattacks against the company/client from the wide array of threat actors;
- Advising on criminal activities that might impact the company's physical and personnel protection operations, as well as its service and product delivery;
- Monitoring reputational and other socio-political risks against the company;
- Conducting due diligence investigations to ensure the resilience and integrity of the company's supply and delivery chains;
- Investigating personnel integrity risks and/or
- Conducting strategic analysis and advising on the company's strategic security management.

The sampling strategy for the quantitative study (Web survey) used non-probability sampling with a blend of convenience, purposive, snowball and targeted sampling by advertising the study through professional associations, personal contacts, social media, LinkedIn and other intelligence analysis related internet interest groups to attract participants from as many countries and variations of employers as possible.

The sampling strategy for the semi-structured interviews was purposive as participants emanated from the survey. The interview pool's size exceeded IPA requirements of between five and eight (ten) participants who have sufficient experience to generate an in-depth exploration of the lived experience of their professional identities and elicit detailed narratives from interviewees. Therefore, the only criterion for the interviewees was that they should have had at least three years of practical experience in the private sector to exclude newcomers who might not be able to relate to the research objectives.

3.6 Ethical considerations

The research study adhered to prescribed ethical procedures and was approved by the University of Portsmouth Ethics Committee. Before completing the survey and the interview, participants were requested to read the information sheet, which outlined

details relevant to the research aims, methodology, use, and data storage. Voluntary informed consent has been obtained from the study participants and confirmed through their completion of the survey and a written consent form (in the case of the interviews). Interviewees gave consent that their interviews could be recorded. They could withdraw their consent during the interview and up till two weeks after the interview. Participants have reviewed their transcripts to ensure that all identifiers have been anonymised. None of the interviewees withdrew from the process.

Confidentiality of personal and professional material shared during the survey and the interview was maintained diligently. On-line survey responses were collected anonymously per the JISC Online privacy policy and security statement. Personal contact information (emails) was only disclosed by participants interested in taking part in Stage 2 of the study. Pseudonyms or anonymous identifiers have been used to present the research findings. Should there have been any concern over possible risks associated with the study, the university's contact details, the supervisor and the researcher were included in the information sheet.

To maximise validity, the researcher had to critically reflect at every stage of especially Study 2, whether her existing knowledge, experience and pre-conceptions influenced the research process. During the interviews, it became apparent that the researcher's embedment in the profession was helpful to elicit personal experiences that would not have been shared were there not a familiarity with the challenges faced by the target group. In the analytical process of the Interpretative Phenomenological Analysis (IPA) study, the double hermeneutic process acknowledged that engaging with the participants' meaning and experiences requires a large degree of interpretation to the extent that the researcher co-construct the lived experience of the participants (Smith, Flowers, & Larkin, 2009). The researcher's reflexive processes (including a journal) and guidance from her supervisors have been crucial to obtaining the maximum scientific validity in the research process.

3.7 Results

In Study 1, 75 respondents to the survey had 16 different nationalities, working in 28 countries with three working globally. As the size of the target group is unknown, the sample size and the diversity of the respondents should be sufficient to attest to the representativeness and generalisability of the findings. The ten participants in Study 2 fulfil the IPA requirements, and they consisted of five males and five females from five different countries.

Chapter 4

Study 1: An exploratory survey on the collective professional identity of SRIA in the private sector

4.1 Introduction

The purpose of the quantitative study into the collective professional identity of SRIA in the private sector was to determine whether people from different contexts self-identify with this emerging professional group and, if so, which aspects or dimensions are shared among the participants. The collective identity of a group of people is defined in this study as both the individual's sense of belonging to a professional group and the group's shared behaviour and values, consciousness or collective action. The more people self-identify or categorise with a specific group, the stronger the collective identity becomes. A strong collective professional identity contributes to shared values and reference frames, leading to better collaboration and communication (Molleman & Rink, 2015).

4.2 Method

Study 1 used an anonymous web-based survey as the data collection method as it was deemed the best option to reach the target population to explore how they perceive and construct their professional identity. Therefore, the survey aimed to obtain valuable information on the target group's demographics and contextual and descriptive data for the study. The secondary aim was to elicit participants for the qualitative interviews in the next study.

A web-based questionnaire is considered the most appropriate instrument to reach a specific population who has access to the internet, is IT literate, and more likely to participate if they know their inputs would be anonymous (Lavrakas, 2008). Internet-based questionnaires have various benefits: they are inexpensive, require minimal effort from the participants and are accessible when the respondents have the time. Furthermore, the study participants' pool can be geographically diverse, as was the case

with this study. Simultaneously, online anonymity encourages honest answers, and questionnaires can be customised so that respondents are guided to different questions depending on previous responses (Hunter, 2012). The survey's online setting allows participants to engage with the questionnaire in their own time and pace in a comfortable and convenient environment.

The main disadvantages of web-based questionnaires are that there is typically a low response rate that ambiguities in the questions could lead to a misunderstanding of survey questions. It is especially true where English is most probably not the first language of some of the target population (Robson & McCartan, 2016). The main ethical concerns in research in this field–the confidentiality of the survey and the anonymity of participants–was addressed through non-invasive and non-sensitive questions and the use of the academic survey platform, JISC Online, which does not collect any identifying metadata.

4.2.1 Survey design

Due to this study's explorative and pragmatic nature, the data collection instrument was developed to obtain as much relevant data as possible across the heterogeneous target population to set the stage for future quantitative and qualitative studies in this under-researched group. It, therefore, adopted a nomothetic approach that gathered both quantitative and qualitative data to explore the professional identity of SRIA in the private sector.

The study drew on existing literature to design the survey questions and relied on previous quantitative studies that developed scientifically sound measuring instruments to investigate several aspects of identity as there are currently no scientifically validated cross-national studies addressing emerging professions' identity. The survey included elements of instruments used in other fields like psychology and counselling (Gazzola & Smith, 2007; Mael & Ashforth, 1992; Verling, 2014; Woo, Lu, & Bang, 2018), organisational studies (Kreiner & Ashforth, 2004), education (Aangenendt et al., 2012; Beijaard et al., 2004), medicine (Liu, Lam, & Loi, 2014; Nikendei, Ben-David, Mennin, &

Huwendiek, 2016), information technology (Brooks et al., 2011) and coaching (Gray, 2011; Gray et al., 2015).

The first part of the survey (Appendix C1) collected demographic details of the participants with questions that dealt with their gender, age, qualifications, employment, nationality, experience in the security risk intelligence analysis field, job title, whether they are in a management position, which sector and type of organisation they are working, fields of analysis/advice and their professional affiliation. Specific demographic details needed to be standardised to ensure uniformity and ease of analysis.

In this regard, the qualification type criteria used were that of the United Nation's International Standard Classification of Education Fields of Education and Training 2013 (ISCED-F) (UNESCO Institute for Statistics, 2015), which classifies education programmes and related qualifications by fields of study according to the broad domain, branch or area of content covered. It was deemed most appropriate to use the UK Standard Industrial Classification–SIC (Office for National Statistics, 2019) to determine the economic sector where the respondents are employed. Most of these questions were closed-ended questions, with an "other" option to disclose information that was not addressed in the predesigned answers. This data enabled the researcher to determine the results' representativeness and map demographic characteristics with data obtained in the second part of the survey.

The second part of the survey consisted of a mixture of a 5-point Likert scale (strongly agree, agree, neither agree nor disagree, disagree and strongly disagree) and open-ended questions. These questions aimed to explore the participants' perceptions of their self-identification, their role and function, the professional challenges they face, their views on the professionalisation and their views on the profession's future. Appendix C2 reflects the research questions that guided the data collection process in the survey.

4.2.2 Validation

As discussed above, this study used elements from other scholars' survey instruments to compile a list of questions that would already have passed scientific validation. No attempt was made to ensure statistical correlation or other validation among the variables and questions. The use of the existing instruments served as a guideline for questions to elicit responses and a baseline for understanding the target group. Most, if not all, elements of collective professional identity, as discussed in Chapter 2, are addressed in the survey based on the model and findings of the research of Bayerl et al. (2018). Their collective professional identity research identified five themes and 18 associated topics used as an assessment or validation tool to ensure that all possible dimensions of the target group's collective identity have been addressed in the research questions in both the survey and the interviews. (Appendix C3)

This study's design process linked Bayerl et al.'s (2018) different collective professional identity themes with the broader research questions. Figure 5 reflects how the survey and interview questions were linked by using colours to depict the different themes people (blue), work (purple), environment (green), valence (yellow) and profession (grey) and arrows to indicate where they are addressed in the survey and interview questions. The validation process followed an inclusive approach by looking at all the possible interpretations of Bayerl et al.'s (2018) themes and linking them with all possible similar outcomes in the instrument questions. As shown in Figure 5, all the themes were adequately addressed in the final instrument design. The study did not aim to assign weights to the different themes to determine the strength (or weakness) of collective professional identity.

4.2.3 Survey piloting

The survey was piloted with four participants from different countries (two from South Africa, one each from Canada and Germany) who were requested to be very critical on the clarity of questions, the sequencing thereof, the time taken to complete the survey, and the number of details requested in the open-ended questions. A request to add a

question on what the participants would think is the profession's future and whether they see a future for themselves in the profession was recommended and implemented.

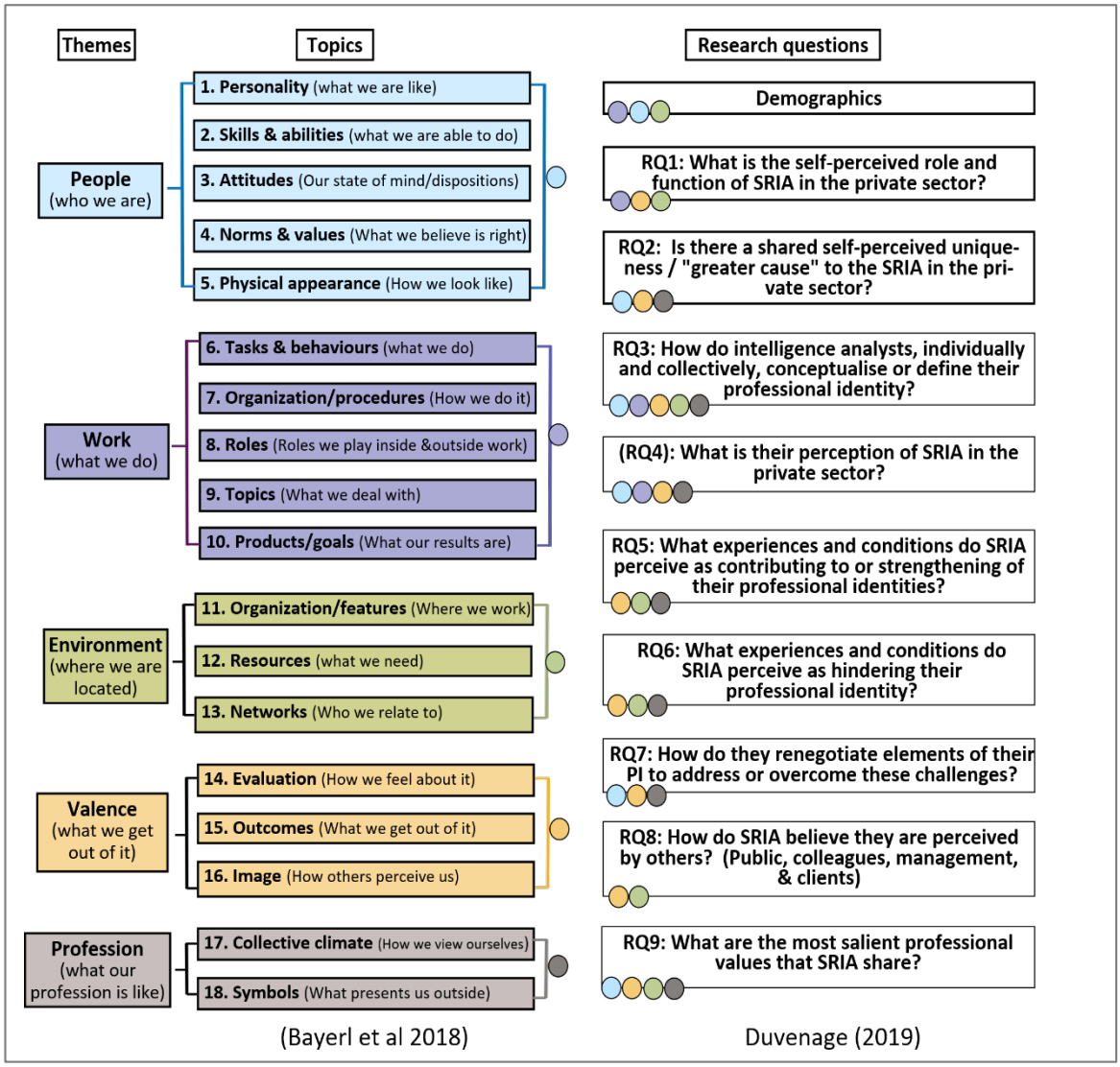


Figure 5: Collective professional identity research instrument design: Bayerl et al.'s (2018) 5 themes for self-expressed collective professional identity (on the left) were used for validation of the study's research questions (on the right)

4.3 Participants

As there is no information available on the actual number of SRIA in the private sector in any country, not to mention the world, the study used non-probability sampling with a blend of convenience, purposive, snowball and targeted sampling to attract as many as possible participants from as many countries and variations of employment contexts. A website was developed, which served as a platform to communicate the researcher's journey and the purpose of the study, elements of the study, contact details, the link to

the survey and a blog. The website was frequently shared on social media to increase awareness of the study and elicit possible participants (see Appendix C4).

The study was also marketed through the following channels:

- Professional associations, like the Association of International Risk Intelligence Professionals (AIRIP), marketed the survey in an email newsletter to their 172 strong membership and during their annual meeting. Simultaneously, the International Association for Intelligence Education (IAFIE - with members across the US, UK, Europe and Australia) also requested their members to market the survey among their students who work in the private sector. The Australian Institute of Professional Intelligence Officers (AIPIO with about 500 members) tweeted the survey link. The Association of Crime and Intelligence Analysts (IACA) also sent out an email to their non-law enforcement analysts (217).
- Twitter: a total of 20 tweets were posted between 1 November 2018 and 31 January 2019, which had 5573 impressions (how many times the tweet was seen on timelines or in search results, with 121 engagements (the total number of times a user interacted with a Tweet).
- Three posts were published on LinkedIn to the researcher's 581 followers, while the study was also introduced to 15 intelligence analysis related LinkedIn groups.
- Email requests were also sent to several private security or intelligence risk companies that the researcher was referred to by people who saw the survey marketing on LinkedIn or Twitter or whom the researcher knew would be willing to participate. These companies were in the US (21), South Africa (1) and Germany (1).

4.4 Procedure

The survey ran from 1 November 2018 to 31 January 2019 on the JISC Online Survey platform that is GDPR compliant and certified to ISO 27001 standard. The fact that the JISC Online tool is reputable among universities in the UK and that the link to the survey

reflected the name of the University of Portsmouth reinforced the study's research nature and provided credibility to the process.

The participants were requested to read the information sheet on page 1 of the survey to understand the study's purpose, the requirements to participate in the study, and related information regarding their data security, confidentiality, the advantages and possible disadvantages of participating. They were also informed that it would take about 20 minutes to complete the survey.

A total of 1220 people accessed the survey, but 1069 left already on the first page where the information sheet was located, 78 left without completing the demographic part of the survey (page 2), while another 27 left at page 3 (which consisted of their role and function). A total of 75 people completed the survey, which is 6 per cent of the initial number that accessed the survey. As the size of the target population is unknown, the researcher had no expectations of the number of people who might participate in the survey. On the last page of the survey, they were invited to participate in the second study (the interviews) by emailing the researcher with a link to her email address that served as a pop-up window with a predetermined subject line "Participation in interviews for your thesis" and "I would like to participate in your interviews for your study of the professional identity of SRIA in the private sector. Please contact me." in the email content.

4.5 Data organisation and analysis

Surveys that include closed and open-ended questions are a good example of using mixed data (Bazeley, 2015), where respondents provide data that could be used for demographic analysis, with comments and contextual information at the same time. Not only do open-ended questions provide useful anecdotes and quotes, but they also provide the opportunity to do a detailed analysis of relationships between the quantitative and qualitative aspects of the data.

The quantitative data in the survey was analysed using descriptive analysis with MS Excel, while SPSS (Version 25) was used for the nonparametric statistical tests to

determine whether the pattern observed during the descriptive analysis could be the same when conducting other statistical analyses. Due to the sample size, certain parameter assumptions for parametric analysis were not met, including that all analysed populations have the same variance.

Nonparametric analysis was found to be sufficient for this exploratory study. The data was re-coded in SPSS (Appendix C5), and two different tests, the Mann-Whitney test (Saunders et al., 2009) and the Kruskal-Wallis H test (Pallant, 2003), were used to determine whether there are similarities or differences in professional identity scales (Questions 16 and 17) and the perception of how others perceive the profession (Question 20) between the respondents according to their demographic characteristics. The Mann-Whitney test determines whether the distribution of scores is the same across the dichotomous independent variables, e.g. gender, management position, professional organisation membership and previous government experience. The Kruskal-Wallis H test (Pallant, 2003) determines whether there is a statistically significant difference between the multinomial independent variables (where there are three or more groups, e.g. age groups, years of experience, qualification level, organisational types, economic sectors and countries).

The survey's seven open-ended questions allowed the participants to share their opinions or voice their perceptions and experience of being a security risk intelligence analyst. The data was sanitised so that only those valid replies (that contained contextual data to analyse) were used for the analysis. A small number of respondents did not complete some open-ended questions, explaining the variance in respondents from the 75 who completed the closed questions survey. The three respondents who work globally were also excluded from the open-ended questions as their responses would have skewed the results where the number of countries in which respondents work was relevant.

NVivo (Version 12) was used to analyse the qualitative data by identifying themes or categories of responses in the open-ended questions and determining the relative frequency of the identified themes. Here it is critical that the researcher, keeping the

research questions in mind, combines the frequency of codes with an analysis of their meaning in context, thereby being mindful of the subtlety and complexity of the issues at hand (Marks & Yardley, 2004).

As the purpose of the research was to determine whether respondents from different countries and economic sectors share perceptions about their profession, the results of the open-ended questions and the country's results and economic sector where they work were imported in NVivo12. The responses were manually coded using mostly inductive coding, which also exposed further dimensions or nuances of the responses that were useful in the analysis. The content was analysed, re-examined and compared until a list of higher-order categories was generated.

Throughout this process, operational definitions were developed for each category and labelled with a code, after which possible themes were identified to categorise the open-ended answers (see Appendix C6). The findings were cross-tabulated in NVivo12 with the country, and economic sector attributes to determine whether there are shared professional identity perceptions across national and economic sector boundaries. The findings were summarised in tables with the frequency for each particular coding category presented as a percentage of all the respondents who provided answers to that specific question and the percentages of the countries and economic sectors in which they work. This enabled the researcher to conduct a descriptive statistical analysis to answer the research questions.

4.6 Results

4.6.1 Demographic analysis

i) Gender, age and experience distribution

The sample of 75 respondents is mostly male (76%), with the majority of males slightly older (45-54 years) than the majority of females (35-44 years), with the most prevalent age group overall is those in the age group 35-44 years old. The spread of years' experience in security risk intelligence analysis was surprisingly wide, with those in the 11-20 years and more than 25 years experience being equal, while those in the 1-5 years

experience and 6-10 years experience slightly lower (see Appendix C7.1). A total of 68% of the respondents are currently in a supervisory role, while the same percentage previously worked for the government and then moved to the private sector.

ii) Geographical representation

The 75 respondents are citizens of 16 different countries across South and North America (Argentina *n*=1, Venezuela *n*=1, the US *n*=29 and Canada *n*=4), Africa (South Africa *n*=11, Botswana *n*=1, Kenya *n*=1 and Tanzania *n*=1), Europe (the UK *n*=13, the Netherlands *n*=1, Germany *n*=4, Finland *n*=1, Greece *n*=1, Slovenia *n*=1 and Bulgaria *n*=1) and South East Asia (Singapore *n*=1). Should the three respondents hold dual or triple citizenship be included in this tally, the total would be 19 different countries' citizenship (the above plus Croatia, Australia and France). A total of 16 respondents (or 21% of the total), all males, work outside their own countries.

The map in Figure 6 illustrates the findings that the 75 respondents work in 24 different countries (those listed above as well as Mexico, Nigeria, Switzerland, Ukraine, Lebanon, and one who works in the US, UK, Australia, Taiwan, China and South Korea), with two respondents working globally without mentioning the countries. An analysis of the different countries represented in the survey, combined from the nationalities and the countries where the participants work, indicates that 27 countries are "represented" in

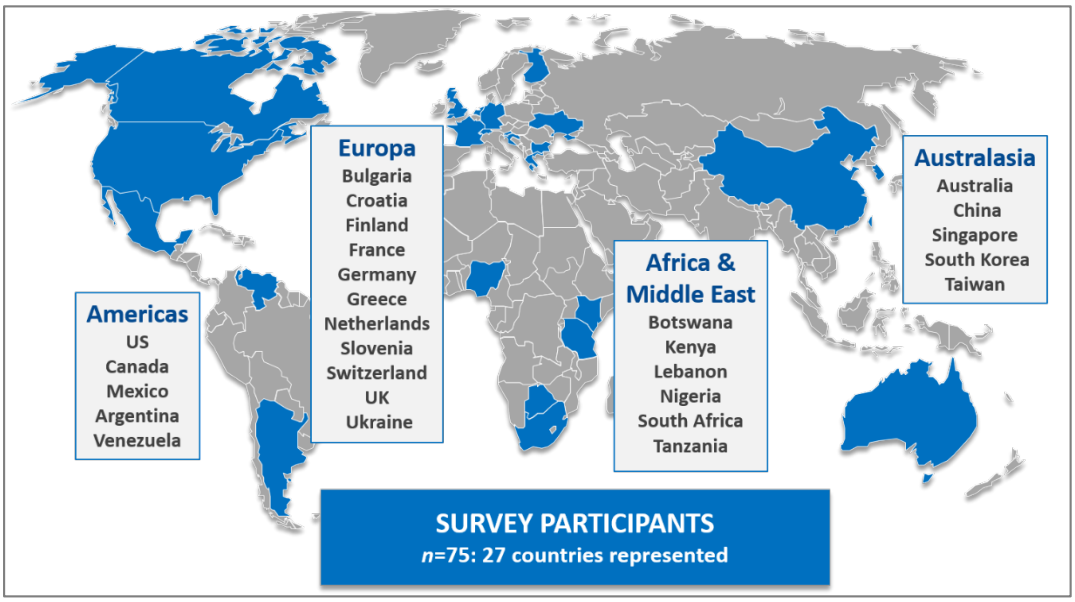


Figure 6: The 27 countries that are represented in the study, with participants with 19 nationalities working in 24 different countries

the survey, which indicates the countries where the function of security risk intelligence analysis is performed.

iii) Qualifications analysis

All the respondents have qualifications ranging from associate degrees/diplomas (1-2 years of tertiary education) to doctoral degrees. The majority of both genders have Masters Degrees; most degrees were attained in the Social Sciences (43%) with the second most qualifications attained in the Services category (15%), which includes security, military and law enforcement (see Appendix C7.2). Other interesting results are that nearly all of those with doctorate degrees are currently in supervisory positions and that those with Master's degrees are well presented in all the age groups.

iv) Job titles

None of the 75 participants had the job title of "security risk intelligence analyst" or "security risk intelligence manager". Only 26 of the 75 (35%) participants had the word "intelligence" in their current job titles, while an additional three stated that their preferred job title should include "intelligence" to suit what they are doing. Only nine (9) of the participants currently had "risk" in their job titles, of which only 3 have the words "risk intelligence" and another three "security risk" in their job titles. Only three stated that another job title that would fit what they are doing included "risk intelligence".

v) Economic sector

The participants are employed across all the private economic sectors (15 in total), where most of them work in the Professional/Scientific/Technical industry (32%). The Finance and Insurance sector has the second-highest presentation with 13% of the respondents, followed by equal representation in the Electricity, Gas, Steam and Aircondition industry, Human Health & Social Work and Information & Communication sectors, each representing 7% of the total respondents (see Appendix C7.3).

vi) Type of employer

Figure 7 depicts the survey participants' distribution according to the type of employer for which they work. Most of the participants (47%) are employed by a private company/multinational corporation or university whose core business is *not* security, where they fulfil a security risk intelligence role. Examples here would be in a pharmaceutical, beverages or technology company. The countries where they are employed are from every continent and thus have the broadest geographical spread (see Appendix C7.4).

The second most, or 16% of the participants, work for local, national or international security risk intelligence consulting companies that provide security risk intelligence and other related services to the private or government sector. Some of these companies would also have embedded analysts in their clients' sites. Participants working in these companies work in Australia, Finland, the Netherlands, South Africa, the UK and the US. The survey did not attempt to obtain the names of employers. However, typical companies in this category would include Calhoun International, Kroll, Control Risks, K2 Intelligence, Stratfor, S-RM, and Tenácitas International, to name a few.

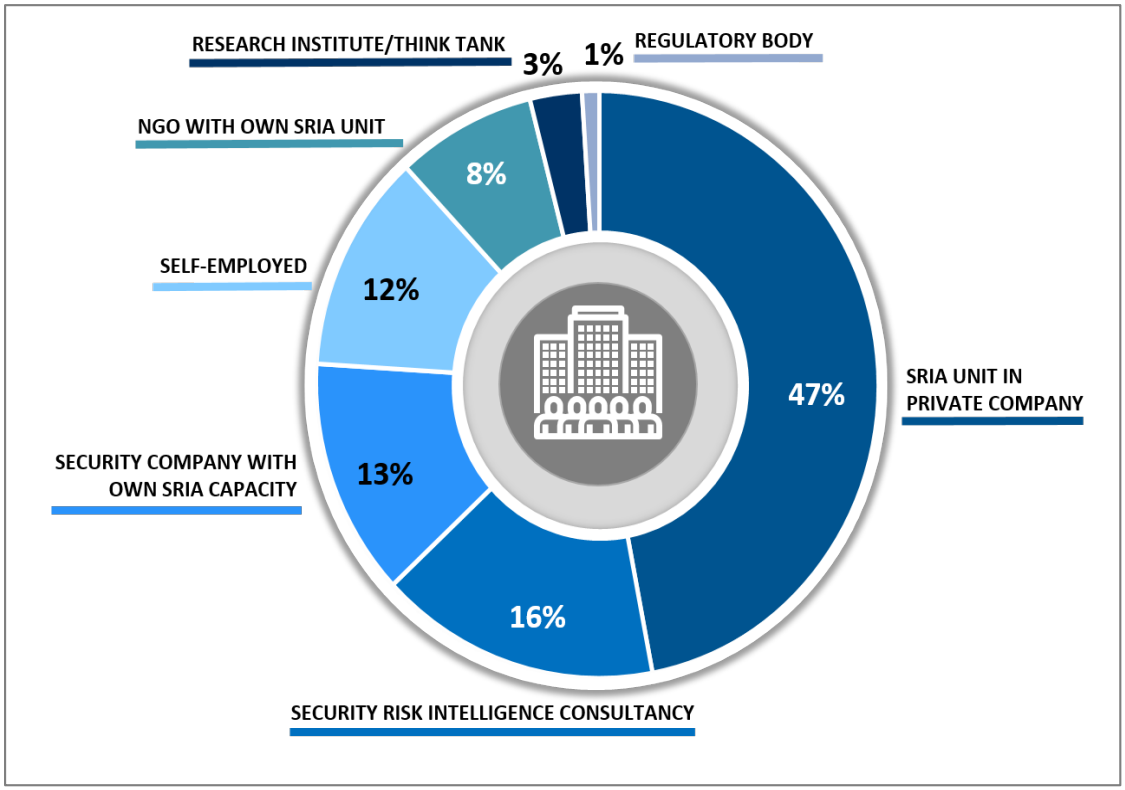


Figure 7: Type of organisations in which respondents work

The third most significant employer of 10 of the total of 75 participants (13%) is private companies who provide the whole spectrum of security services, including guarding, investigations and security systems but which also have their own security risk intelligence analysis capacity, are mostly from Nigeria, Ukraine and the US. Companies that would typically resort under this category would include Securitas, GardaWorld, G4S and Pinkerton.

Interestingly, 12% or nine of the respondents are self-employed, which would imply that their specialist knowledge and business know-how provide good entrepreneurial opportunities in this field. They are working in South Africa (5), Germany, and the US, while two work globally. Fewer respondents are employed by non-governmental organisations (NGO's) with their own security/risk intelligence capacity (8%), research foundations or think tanks that provide intelligence advisory services to clients (3%) and lastly, regulatory bodies (1%).

vii) Analytical focus areas, deliverables or advice to clients

The respondents could choose multiple answers to indicate the type of analysis and/or threats they advise regularly. It was evident from the survey results that SRIA monitor or focus on multiple disciplines or threat areas simultaneously in the execution of their functions (with a mean of 4.4 different focus areas), and not only on one or two areas like their counterparts in the national security or law enforcement sectors (see Figure 8).

Appendix C7.5 illustrates how the different focus areas were grouped in broad categories to enable in-depth analysis of the variety of topics SRIA in the private sector have to research, analyse and provide advice. The category focus area that most of the respondents conduct research and advise on is Analytical Practices (a mean of 51%).

Although further details have not been elicited in this part of the survey on what this entails, it most likely refers to integrating different analytical methods in deliverables to get their message across. It has become common in the intelligence analysis field to explain the analytical methodology to clients to strengthen credibility and instil rigour in the analysis process.

The second most prevalent category is that of Security Management (48% mean), followed by Protective Intelligence (42% mean), Geostrategic and Political Intelligence (39% mean), Crime Intelligence (35% mean) and lastly that of Cyber Intelligence with a mean of 24% of the respondents. When the single most prevalent focus areas are identified, the majority (more than 50%) of the respondents deals with security risk management (71%), strategic analysis & foresight (64%), geopolitical developments (63%), followed by general crime (59%), travel risk (57%), security management strategy (55%), terrorism & counter-terrorism (53%), with personnel security incidents and reputational risks both at 51% of the respondents.

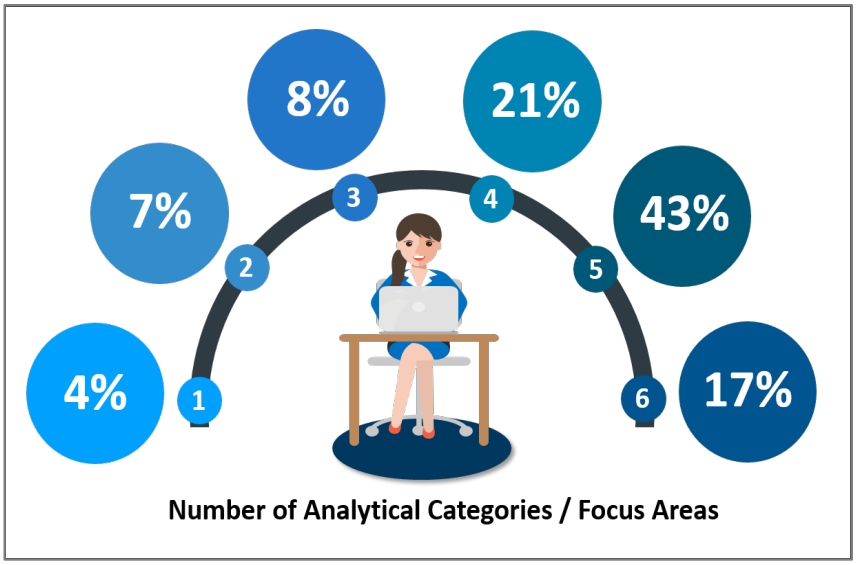


Figure 8: The workload of participants according to the different analytical categories or Focus Areas that they are responsible for in advising and providing deliverables: n=75

viii) Professional organisation membership

The purpose of including membership of professional organisations in the survey was to determine whether SRIA deliberately associates themselves tangibly and more officially to the collective self-identification with others in the field. The majority of the respondents are members of professional organisations (69% against 31% who are not). This analysis's age distribution was interesting: those in the 25-44 age groups were less prone to be members of professional organisation than those in older age groups–on average 63% against 88%. Those older than 44 years are overwhelmingly members of

professional organisations, with between 80% and 100% of the respondents in that age group. The anomaly is the two respondents in the age group 18-24 who are both members of a professional organisation (see Appendix C7.6 and C7.7).

The survey indicated that most supervisors (84%) hold professional organisation membership, while only 50% of those in non-supervisory roles belong to professional bodies. The reason for this result might be more complex than making a sweeping statement like "when you are a member of a professional organisation, your chances for promotion are better". The nature of the work indicated that networking and stakeholder management are essential for success in this profession.

Membership of professional bodies enables more extensive networking (34% of those who hold membership of professional bodies state networking as a reason why they are involved). The other reasons for belonging to a professional organisation are in order of frequency are "information sharing" (20% of responses), "benchmarking of best practice", and "learning and professional development" (both at 18%), while on 8% mentioned "certification and professional recognition", while 2% stated that their company requires it. One respondent replied that he/she sees no value in being a member of a professional organisation.

The main reasons given by the 23 respondents for *not* belonging to professional organisations can be grouped into four categories in order of frequency. Firstly, they do not feel they need it (50%) with comments such as "it doesn't appeal to me", "it's not necessary for my job", "they feel outdated", "I have sufficient qualifications and don't need professional designations". Secondly, there is a lack of awareness of relevant professional organisations (30%) from Canada, the US, South Africa and Tanzania – which is surprising because one would have assumed that at least Canada and the US analysts are exposed to professional organisations. Some of the remarks in this category included: "no existing organisation for the private sector", "one exists?" and "never occurred to me".

Thirdly, 16% of the respondents stated that the cost is too high compared to the perceived membership benefits. When comparing the respondents' professional

organisation membership with the qualification level, it is clear that those with higher qualifications are also more likely to belong to professional organisations (see Appendix C7.7).

The majority (78%) of all respondents who have Masters' degrees belong to professional organisations. At the same time, the mean of the number of memberships is also higher in this group (1.9) while those with Doctorate degrees have a mean professional organisation membership of 1.8, compared with those with lesser qualifications, i.e. Honour's degrees (0.9), Bachelor's (1.4) and one or two-year qualifications (1.3) mean.

The professional organisations to which the respondents belong could be categorised into two main groups: those professional organisations that provide opportunities for knowledge sharing, networking AND certification (*n*=20, see Appendix C7.8), while the other group was those organisations that do not offer certification or professional development opportunities, but are mainly collaborative networks with a code of ethics or professional standards and/or standards for affiliation by educational institutions who underwrite their objectives (*n*=23, see Appendix C7.9).

Due to the wide selection of sectors in which the respondents work, the professional organisations to which they belong range from risk intelligence or security management organisations to specialised organisations dealing with, for instance, university security or business continuity. The most global membership professional organisations are the Association for International Risk Intelligence Professionals (AIRIP) and ASIS, with 14 members each work in 19 different countries or 68% of the 27 different countries.

4.6.2 The perceived role and function of SRIA

The survey question "In your experience, what is the main role and function of SRIA in the private sector?" aimed to obtain the self-descriptions of the tasks of the target group of SRIA in the private sector. Three distinct themes of tasks were identified with the majority (78% of the 73 respondents and 83% of the 24 countries and 100% of the economic sectors represented) emphasised that their responsibility is to provide forewarning and situational awareness of the threats to the business (see Table 1).

A closer look at the data indicates that the second role—to support the decision-maker—is a customer-centric perspective of the primary role and function of providing forwarning and situational awareness. The third most mentioned role, the provision of security risk management functions, relates to the methodology or craft applied to execute the primary role and function of forewarning and situational awareness.

An interesting finding is that those analysts working for a security company with its own security risk intelligence analysis capacity preferred the function of "assisting and supporting consumers to make sense and better decisions" more than the other two functions. They might be more involved in operational matters where they assist investigators than those analysts working for other types of organisations.

Table 1

The role and function of SRIA: n=73

Themes and typical quotations for defined themes	% of respondents whose answers included a code in the theme	% of countries whose answers included a code in the theme: *n*=24	% of economic sectors whose answers included a code in the theme: *n*=15
Provide forewarning by identifying & analysing threats and risks to business	**78%**	**83%**	**100%**
"Anticipating and mitigating risks and threats to the corporate world."			
"To provide strategic forecasting intelligence to help guide Company decisions and advise on tactical and operational events that may impact the Company's people, assets, or reputation."			
"To make the company aware of security and political risks which threaten the security of personnel & key assets as well the viability of ongoing or future business."			
Assist & support consumers to make sense and better decisions	**36%**	**50%**	**80%**
"Assist consumers to make sense of the past and the present."			
"To provide stakeholders and decision-makers reliable, accurate information layered with astute assessment to enable them to make business/security decisions."			
"To bring expertise to business owners and executives to make informed decisions. By quantifying and identifying risks, analysts provide insight into business operations and provide risk information for business executives."			
Provide risk management advice	**32%**	**50%**	**60%**
"Monitor and assess risks to the business, alert the business to emerging or escalating risks, recommend risk mitigation measures."			
"Enable efficient business functions through the proactive identification of applicable risks so that the proper assessment, mitigation, and acceptance of any residual risk can be undertaken."			
"Extensive research and analysis and designating each risk with a risk level (typically 'high', 'medium', or 'low') through use of a risk matrix (impact of event happening vs likelihood that it will happen) along with their own comment on whether they think the risk is worth taking and they should invest/travel there or whatever it is they needed the risk assessment for."			

4.6.3 The perceived unique contribution of SRIA to the private sector and to society

It is evident from the responses to the question "What is the unique contribution that you bring to the private sector and society?" that respondents had very similar replies to what they have given in the previous question in terms of their role and functions. The purpose of the question was to determine whether they share a perception of the unique value or impact (Bielska & Pallaris, 2017) they bring to the corporate world and

society. As this was an open-ended question, participants offered multiple answers see Table 2.

Just more than a third of the respondents (37%), which represented 45% of the countries and 67% of the economic sectors represented in the survey, stated that their specialist knowledge helps identify and prevent threats to their company, the sector, and the society as a whole. In a similar vein, the second most prevalent theme is that of supporting decision-makers (35% of respondents, 80% of the countries and economic sectors represented) to make better-informed decisions that would assist business, and in some cases, "improve investments in developing and post-conflict countries that can improve societal conditions".

The third highest response rate to the question was that of "to enable a safe working environment, risk reduction & loss prevention for companies & industries that contribute to national economies" which a slightly lower percentage of the respondents (32%), but still 50% of the countries and 73% of the sectors represented in this sample offered as their contribution. An interesting minority view is that of four respondents from South Africa and the US from the Professional, Scientific and Technical as well as Information and Communications sectors, that stated that "they augment government capability to understand security risks to deliver stability" and that they "provide a service that the government and law enforcement cannot provide due to a lack of resources or different focus".

This question's overall results show a relatively equal distribution of viewpoints on the unique contribution they bring to society and that the viewpoints are directly related to the role, and functions discussed previously. The three identified themes share a common purpose: protecting or defending the company's interests, clients, and society, which indicate that they feel their profession is meaningful and purposeful.

Table 2

The perceived unique contribution or value of SRIA: n=71

Themes and typical quotations for defined themes	% of respondents whose answers included a code in the theme	% of countries whose answers included a code in the theme: *n*=22	% of economic sectors whose answers included a code in the theme: *n*=15
Provide insight into threats to a business, sector, industry or national security	**37%**	**45%**	**67%**
"The ability to apply unique industry insights towards threats."			
"To allow organisations (and their communities) to be proactive against risk and improve resiliency."			
Enable more informed decision-making	**35%**	**68%**	**80%**
"An informed point of view that can be objectively applied towards business decisions."			
"We are able and experienced in providing honest assessments to those in positions of influence and are therefore able to enable business in environments which would not otherwise be accessible. In the developing world and post conflict countries, this can bring great investment which can improve societal conditions".			
Enable a safe working environment, risk reduction & loss prevention for companies & industries that contribute to national economies	**32%**	**50%**	**73%**
"Mitigate losses for major private corporations, which contribute significantly to national economies."			
"We help foster a secure work environment - ensuring our physical job sites are safe, our colleagues are appropriately vetted, and our travellers are educated on security trends worldwide. This fosters a productive and safe workforce on a global level."			
"Ability to advise the business of the potential emerging threats which will, in turn, contribute to the protection of the business assets and its people."			

4.6.4 The perceived benefits/opportunities that respondents derive from being a SRIA in the private sector

The survey question on the benefits respondents derive from the profession aimed to determine which experiences or conditions strengthen their professional identity and whether they share the same viewpoints. In essence, the question targeted the meaning or value the profession holds for its members, as self-interest (and a positive self-image) is the primary determinant for self-categorisation with a group or profession. Membership of social groups, like professions, are associated with positive or negative value connotations (Tajfel & Turner, 2004). The analysis of this specific open survey question was done deductively, applying the three themes in Bayerl et al.'s (2018) "valence" factor to determine what the respondents "get out of" being SRIA. Valence in

psychology indicates the subjective value or intrinsic attractiveness (positive valence) or aversiveness (negative valence) of an event, object, person, or situation (N Pam, 2013).

The themes are 1) the personal, concrete examples of what they gain by being in this profession, 2) image – or the standing the profession gives them inside and outside the professional group and 3) the value of the profession in their own eyes or their evaluation of being in this profession. The sub-themes were inductively determined based on the replies of the respondents.

The analysis indicates that the respondents derive not many common benefits from being in this profession. The most common benefit—that of them valuing the intellectual stimulation of the job—was only mentioned by 51% of the respondents, although they are working in 55% of the 23 countries and 73% of the 15 economic sectors represented by the respondents. No specific demographic commonalities or differences could be detected as the responses were equally spread across demographic and sectoral boundaries (see Appendix C7.10).

Most of the respondents (80%) identified personal benefits, with the majority (51% of all participants, 55% of the represented 23 countries and 73% of the 15 sectors) stating that they enjoy the work's intellectually stimulating nature. Comments such as the one hereunder reflect that the respondents value the fact that they are intellectually challenged to fulfil their primary role and function of staying abreast of new developments that could impact their organisation.

> "I have been in this environment for twenty years, and not one day is the same. I enjoy working for and with different people. All my clients have different requirements and needs, and it is great to work on a diverse range of topics."

Many also reflected that they are continuously developing new skills like "I have the opportunity to do extremely interesting work and the potential to constantly learn." The second most common sub-theme in personal benefits with 47% of the 15 economic sectors represented, is that the profession provides them with the opportunity to know and understand what is happening in the world, much more than other people, which is

good for their self-esteem with comments such as “I see what is over the horizon before others”.

The second theme, the profession's image, was mentioned by only 17% of respondents that represent 53% of the economic sectors. Comments such as “My clients recognise me as a valuable expert”, “the profession is considered prestigious by co-workers”, “I have access to decision-makers” and “I have management’s attention” emphasise that at least 13 of the 71 respondents to this question value the good image the profession offers them personally. The value of being recognised by their peers are slightly higher than the value they place on being recognised by their management.

About a third of the respondents mentioned the third theme of Bayerl et al.(2018), namely the profession's self-perceived value. For most of these, the fact that they have an impact on business (53% of the economic sectors) such as “the ability to influence large-scale strategic business decisions and projects” and “forming part of an organisation's early warning system along with other executives” is a crucial benefit they derive from being in this profession. 11% of the respondents feel that they are “making a difference” or “have the opportunity to help others with difficult problems”.

4.6.5 The perceived challenges of being a security risk intelligence analyst that could impact on their professional identity

The respondents had to offer at least three challenges they face as SRIA in the private sector that might impact their resilience to develop and maintain their professional identity. This question is relevant to determine whether the respondents share the same challenges across nationalities and economic sectors and, where possible, recommend systemic recommendations to address these challenges. Challenges in the workplace serve as cues to professionals to rediscover whether they want to remain in this profession and, if so, strengthen their resolve or commitment to their professional identity by finding ways to minimise or circumvent the impact of these challenges through identity work.

The results of the survey of this question were analysed inductively. Four main themes were identified: 1) those challenges they face that are stemming from their task as SRIA, 2) challenges that are related to the organisational context in which they function, 3) challenges relating to the broader environment, and 4) the challenges related to their experience of the profession itself. It has to be kept in mind that respondents might experience similar challenges than others but might not have put it in the top three of their most pressing challenges. Should they not have been limited in their responses, the similarities and difference could have been even more interesting (see Appendix C7.11).

The challenges faced by most of the respondents are those related to their working environment (theme 2), with 80% of the respondents representing 92% of the countries and 93% of the economic sectors, citing a total of 12 challenges. The most common workplace challenge that respondents share across national boundaries and economic sectors is a lack of understanding about the value and purpose of security risk intelligence analysis in the organisation they work. More than half of the respondents (54%) across a third (67%) of the countries and 80% of the economic sectors stated this as one of the main frustrations in their workplace.

The most interesting finding relates to the variable of the different type of organisation where 80% of those working in private security companies said there is a lack of understanding of intelligence analysis. In comparison, those working in private companies whose core business is not security had 51% stating the same, while those working for NGO's (50%), are self-employed (44%), and even working for security risk companies (41%) feel that their function is misunderstood. Statements included "it is difficult to combat the narrative and misperceptions of intelligence", or "helping business partners to understand that this is not a crystal ball", "clients or partners are not listening to advice or analysis and doing their own thing, or they do not want to make a decision", "my company discounts sound intelligence and then complains they were not informed", "the function is seen as a necessary cost rather than contributing to the financial success of the company" and "it is a challenge to educate leaders on what the Security Risk Intel Analyst can bring to the table".

The second most shared challenge is that of lack of resources (27% of all respondents, 25% of all countries represented and 60% of the economic sectors, with the highest percentage of 58% from respondents working in private security risk companies), with the lack of funding and access to information the main challenge. Furthermore, it seems as though most of the economic sectors struggle with a lack of human resources support (60% of the economic sectors, 33% of the countries represented and 23% of the respondents). The main identified issues relate to the fact that the HR personnel do not know what the functions of a SRIA are, with resultant mismatched recruits. Furthermore, analysts' lack of career pathways is also perceived to be a challenge, especially in private sector companies whose core business is not security (34% of the respondents in this type of organisation).

Other noteworthy challenges include the counter side of the main benefit of being a security risk intelligence analyst in the private sector–an intellectually challenging career–where nearly a quarter of the respondents and countries, and 60% of the economic sectors stated that they experience information and cognitive overload. Some of the comments here included "Small teams with large workload leads to high analyst

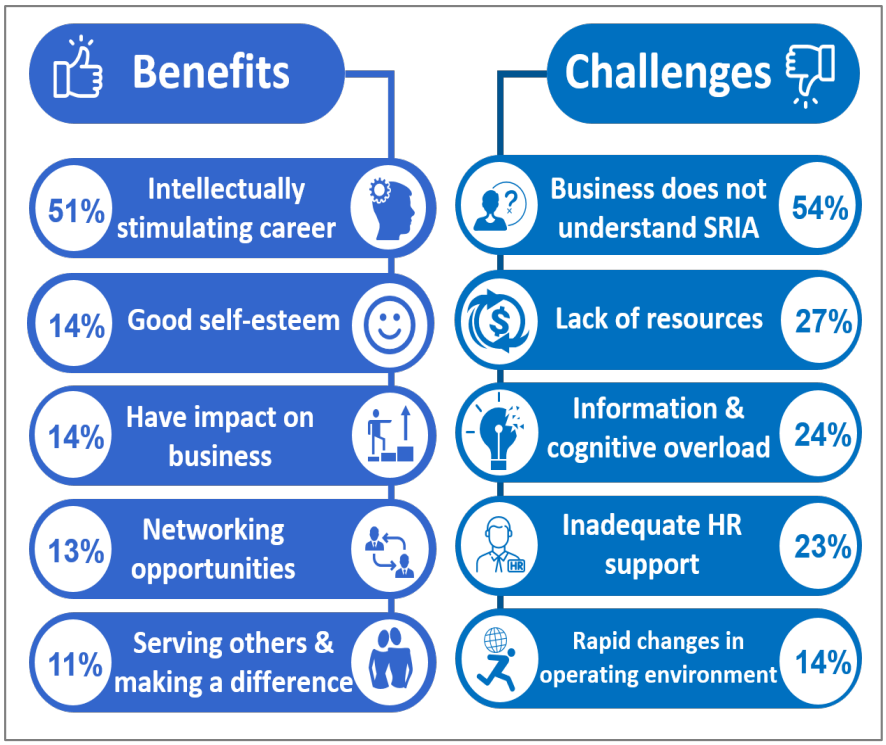


Figure 9: The five highest rated benefits and challenges of being a Security Risk Intelligence Analyst in the private sector

turnover and high burnout rates", "the rapid change of the geopolitical landscape and open source intelligence collection methods", "very expansive priorities, difficult to become expert in all facets" and "I have to keep constantly up to date with geopolitical developments across the world. Everyone expects you to be an expert on geopolitics in every country."

A third of all the economic sectors represented find time pressures challenging when conducting their tasks. Some of the comments included "people do not understand that it takes time for a good research product" and "little time to learn on the job due to competing priorities". A further challenge related to their function is the lack of cooperation and information sharing with other departments in the same organisation across 33% of the economic sectors. Figure 9 depicts the five highest rated benefits and challenges of being a Security Risk Intelligence Analyst identified by the respondents.

4.6.6 Values shared by SRIA in the private sector

The purpose of including a question on the three most important professional values or ethical standards to which the respondents execute their task was to determine whether values or norms were shared across national and sectoral boundaries. The issue of ethics and morality in the private security sector, vis-à-vis that of the formalised ethos found in the intelligence community, police or military, has received attention in the last few years (Bean, 2015; Franke & Von Boemcken, 2009; Voelz, 2009).

These studies found that the notion that private-sector employees would forfeit all other values for profit was misplaced and unfair due to the internalisation of common ethical standards and professional values by the vast majority of private security employees. Many values are universal and transversal across multiple professions, such as integrity and honesty, reflecting the individual and professions' aim to contribute and positively service society.

From the inductive analysis results, it is clear that the respondents do not experience major ethical dilemmas that might impact their commitment or loyalty to their companies. Only one respondent remarked that he had been tasked to do something

unlawful, which he refused to execute. There was no indication that respondents experienced tension between their values and the profit objective of their companies. Their stated values were taken at face value and were not changed if they were to use integrity *and* honesty as they perceive these to be two different, although related, concepts that they associate with.

Four main themes emerged from the inductive analysis of the 71 respondents to this question, related to their personal (in-ward looking) values, those values that guide them when they execute their task, those values which guide them in their work environment and those values that guide their interaction with other people (see Appendix C7.12 and Figure 10).

The most common theme was "personal values", which represented 80% of the replies, 83% of the countries and 73% of the economic sectors represented. The most shared value in this theme was that of "integrity", which 52% of the respondents followed, followed by "honesty". One respondent remarked, "A rock steady - even keel personality - we are the calm in the crisis", "honesty before sales", and "I always tell the truth. You can ask me anything as long as you are not afraid of the answer." Respondents who work in NGO's, in companies whose core business is not security, research institute and self-

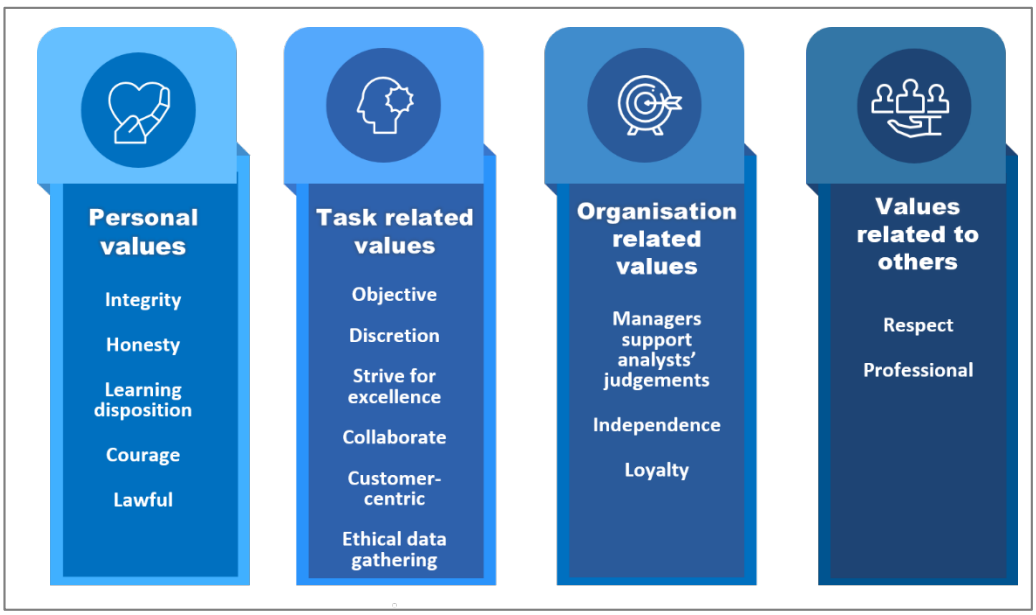


Figure 10: The four main values themes identified in the survey

employed respondents offered these personal values most often as the values according to which they function in the workplace.

The second most prevalent theme was those values that dictate how they perform their task, which was mentioned by 72% of the respondents. The most commonly shared value here was "objective" with 34% of the respondents, across 50% of the countries and 73% of the economic sectors, with comments such as "objective analysis is non-negotiable" and "remove bias as much as possible from the end product". The second most prevalent value in this theme was using discretion in dealing with clients, stakeholders, and sources of information. Those dealing with sensitive sources or projects commented: "trust - we have to keep secrets" and "I have to maintain confidentiality when necessary". The values of respondents who work in security risk intelligence consulting companies, private security companies, and research institutes and think tanks were more task-oriented, especially valuing objectivity, discretion, and striving for excellence higher than other values.

The third and fourth themes, namely those values that their organisation espouses which they agree with and those values that govern their dealings with other people, both represented only 10% of the respondents, but still a sufficient commonality among the different countries (25% and 17%) and economic sectors (33% and 27%) to confirm that there are shared values across the spectrum.

4.6.7 Collective professional self-categorisation and self-identification

Self-categorisation is regarded as the heart of collective identity and a precondition for other collective identity dimensions (Ashmore et al., 2004). Survey question 16 aimed to determine whether the respondents, individually and collectively, self-identify with the security risk intelligence analysis profession. The nine questions measured their need for professional identification and self-categorisation with the profession and their emotional attachment to the profession.

i) Analysis of results of all respondents combined

After the reverse coded item was rectified, the overall results for this part of the survey show that the majority (74%) of all the respondents self-identify with the security risk intelligence analysis profession with a median of 43% that strongly agree with the statements and 31% that agree across all nine related statements with a standard deviation of only 0.91 and a mean of 1.95 (Agree) (see Appendix C7.13 and Figure 11).

When combining the "strongly agree" with the "agree" results (positive perception) and the "strongly disagree" with "disagree" (negative perception) with "neither agree nor disagree" indicating a neutral perception, the results were:

- 85% feel that their personal goals, values and beliefs overlap with that of the profession;
- 93% would regard themselves as part of the in-group by using "we" rather than "I" when talking about the profession;
- 68% explicitly define themselves as a security risk intelligence analyst professional with 20% being neutral;
- 74% are interested in what others think about the security risk intelligence analysis profession;
- 96% of the respondents are positive to socialise with colleagues to share best practice;
- 60% stated that it feels like a personal compliment when someone praises the profession, with 33% being neutral;
- 73% stated that they are interested in what others think about the profession;
- In the question, whether they would feel embarrassed when the profession is criticised or negatively portrayed in the media, the response was more evenly distributed: 33% answered positively, 35% was neutral, and 31% negative.
- 65% stated that they would instead search for another employer than to change their profession, with 16% neutral and

- 76% agreed that it is more important for them to conduct their work professionally than being a member of a specific "profession", with 11% being neutral.

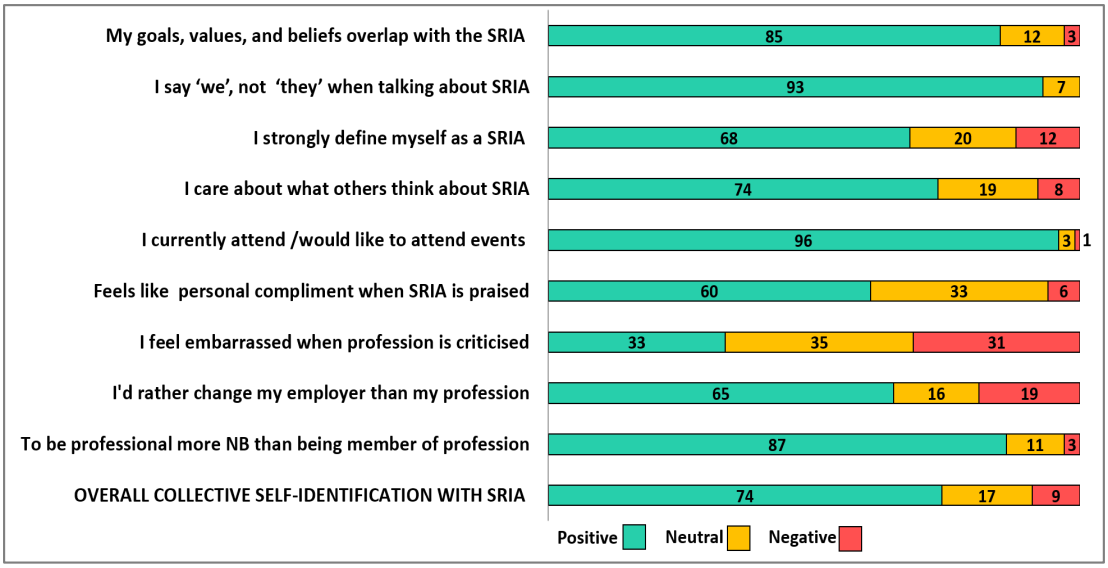


Figure 11: The collective self-identification and self-categorisation with the security risk intelligence analysis profession

ii) Analysis of results per demographic variable

The research questions required that the elements of self-categorisation in the survey are compared with the demographic variables by using non-parametric tests (Mann-Whitney and Kruskal Willis tests) in SPSS to determine whether there was any significant statistical similarities or differences with professional identity elements across the genders, type of organisations, countries, and economic sectors. Overall, there was a similar distribution across the different demographic elements, confirming that most analysts share the same professional identity elements of self-categorisation (see Appendix C7.14). However, from this data, it can be concluded that the following instances had statistically significant different distributions (meaning that the respondents have significantly different opinions about a particular issue):

- It is more important for males than females ($U=334$, $p=.013$) and for managers ($U=443$, $p=.031$) to be professional in their work than being a member of a specific profession;

- Not all respondents would like to attend events where security risk intelligence analysis best practice is shared. People with previous government experience are less likely to attend than those without prior government experience (U=444, p=.014). Respondents in the agriculture, mining, finance, public and health sectors are more likely to attend these events than the other sectors.
- People who are in management positions are more likely to feel embarrassed when a story in the media criticised the security risk intelligence analysis profession than those who are not in a management position (U=412, p=.020)

Although the statistical difference between the type of organisations for whom the respondents work were negligible, it was interesting to note that there was only a .6 difference in the mean between those who self-categorise the most with security risk intelligence analysis as a profession (research institutes or think tanks with a mean of 1.61) and those who least self-categorised with the profession (those who work for independent regulatory bodies with a mean of 2.22).

4.6.8 Collective self-perception of the security risk intelligence analyst profession

i) Analysis of results of all respondents combined

Survey question 17 measured how the participants perceive the security risk intelligence analyst profession. After the reverse coded item was rectified, the results show that the majority (75%) of all the respondents have a good perception of their profession, with a median of 36% that strongly agree with the statements and 39% that agree. The five related statements reflect a standard deviation of only 0.87 and a mean of 1.75. When combining the "strongly agree" with the "agree" results (positive perception) and the "strongly disagree" with "disagree" (negative perception) with "neither agree nor disagree" indicating a neutral perception, the results (see Figure 12) were:

- 84% think highly of the security risk intelligence analyst profession with no negative perception and 16% being neutral on the issue;
- 68% consider it prestigious to belong to the profession, with 25% being neutral and 7% having a negative perception. The same percentage defined themselves as SRIA in the previous question.

- 74% of the respondents consider the Security Risk Intelligence Analysis profession to be one of the best professions for people with the relevant skills and education;
- 75% stated that they would recommend the career to someone else;76% of the respondents were positive when asked whether they see a future for themselves as a Security risk intelligence analyst and would like to remain in the profession in some capacity.

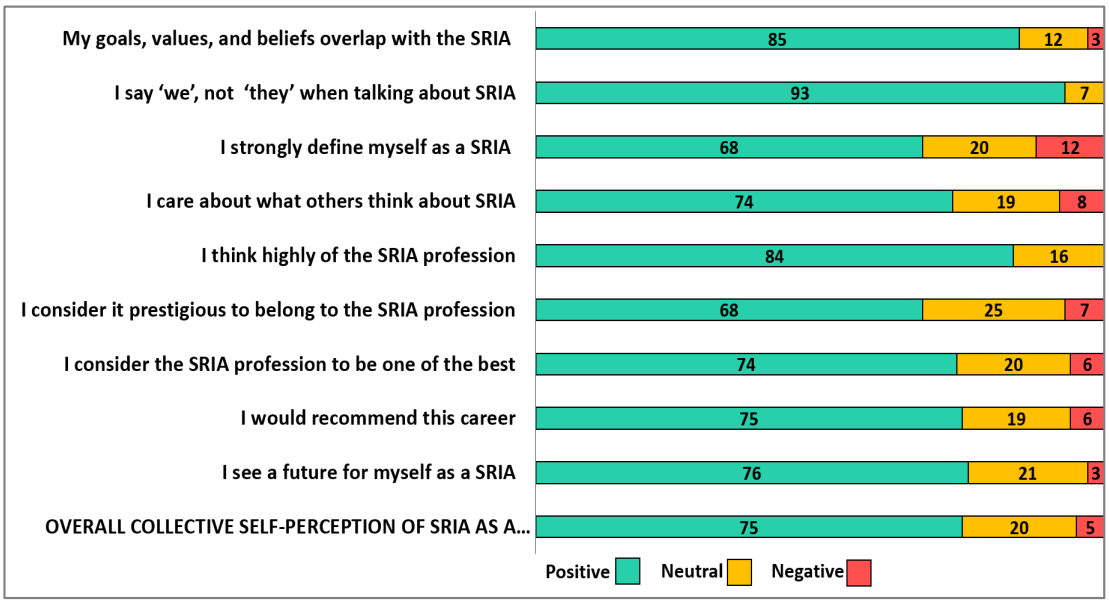


Figure 12: The collective self-perception of the security risk intelligence analysis profession in %

ii) Analysis of results per demographic variable

The research questions required that the elements of collective self-perception in the survey are compared with the demographic variables by using non-parametric tests (Mann-Whitney and Kruskal Willis tests) in SPSS. The purpose was to determine whether there was any significant similarities or differences to this specific professional identity element across different demographic variables, including genders, type of organisations, countries and economic sectors.

Overall, there was a similar distribution across the different demographic elements, confirming that most analysts share the same professional identity elements of self-perception of their profession. Only one out of the five sub-elements from self-perception had statistically significant different distributions (meaning that the

respondents have significantly different opinions about a specific issue). The data (see Appendix C7.15) showed that the respondents do not agree that they consider the security risk intelligence analyst profession one of the best professions for people with the relevant skills (H=11.712,p=.039). Further to this, the analysis shows the following:

- People with more years experience (21 years and more experience and those with less than five years experience have a less positive perception about it being "the best profession" than those with 6-20 years experience. The group that perceives the profession as one of the best are those with between 11 and 15 years of experience.
- There were broad differences in the economic sectors when they answered this question. The agriculture, mining and health sectors are much more favourable than those in the professional, manufacturing, wholesale/retail, electricity and accommodation, which are the least positive.
- Respondents in a management position are more likely to think that security risk intelligence analysis is the best profession for people with a specific skill set than those not in a management position.

When comparing the means of self-perception between the different type of organisations for whom the respondents work, there is a difference of 1 between the respondents who are the most favourable towards the profession (NGO's at 1.6 mean) and those who are the least favourable towards the profession (those working for independent regulatory bodies at 2.6 mean).

4.6.5 Collective perception of how others perceive the security risk intelligence analyst profession

i) Analysis of results of all respondents combined

The survey results that dealt with how the participants view others' perception of their profession are more ambivalent than the previous two results. After the reverse coded item was rectified, the results show that 48% of the respondents think others have a relative good perception of their profession, with a median of only 10% that strongly agree with the statements and 38% that agree. The neither agree nor disagree median

is 34% which illustrates the high level to which the participants lack an opinion on how others perceive their profession, with 18% perceiving that others perceive their profession negatively. The five related statements reflect a standard deviation of only 0.90 and a mean of 2.63.

When combining the "strongly agree" with the "agree" results (positive perception) and the "strongly disagree" with "disagree" (negative perception) with "neither agree nor disagree" indicating a neutral perception, the results (see Figure 13) were:

- 44% of the respondents think that others, in general, think highly of the Security risk intelligence analyst profession, while 41% is neutral on the issue and 16 are negative about the statement;
- 47% perceive that others think it is prestigious to belong to the profession, with 41% being neutral and 12% perceiving that others do not think it is prestigious;
- Only 21% of the respondents believe that others consider the Security Risk Intelligence Analysis profession to be one of the best professions, with 49% having no opinion and 29% perceiving it to not being considered as prestigious by others;
- The highest positive perception of others is that of the participants' stakeholders who are perceived to value their contribution to achieving the organisation's mandate (80%), with 15% being neutral and only 5% believing that their stakeholders do not perceive their contribution positively.

- A thought-provoking result is that the participants' management and/or clients are perceived to be less appreciative of the profession (51%) than the stakeholders (80%), as discussed above. 21% were neutral, while 28% perceive their management to have a good perception of the profession.

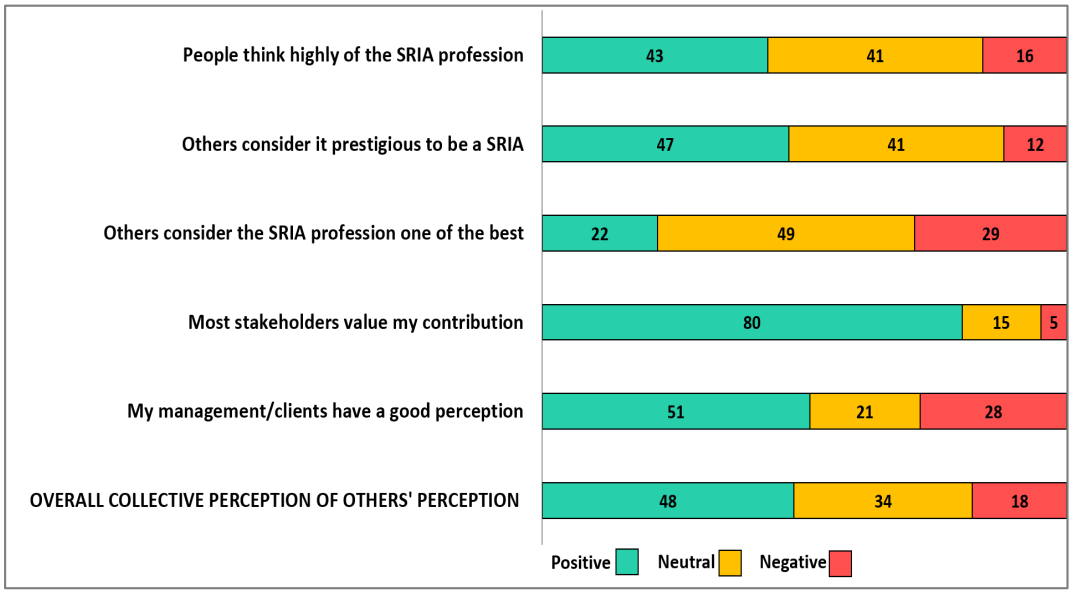


Figure 13: The collective perception of others' perception of the sria profession in %

ii) Analysis of results per demographic variable

Again, the research questions required that non-parametric tests (Mann-Whitney and Kruskal Willis tests) be used to determine to what extent there is a difference across demographic variables in how the respondents think others perceive their profession (see Appendix C7.16). In general, there is an equal distribution across the demographic variables except in the age groups where it was clear that age was the primary determinant where people had statistically significant differences about how others see the security risk intelligence analyst profession (H=11.580, p=.041). It seems as though the older respondents are, the more cynical they are about how others perceive the profession. Those who stated that people, in general, do not think highly of the profession are in the 65 and older and 45-54 age groups. In contrast, those between 18-34 years are much more optimistic about how other people, in general, think very highly of the security risk intelligence analysis profession.

4.6.6 Suggested strategies to strengthen and improve the professional identity of SRIA

In an open-ended question, 61 of the respondents offered suggestions on how the professional identity of SRIA in the private sector could be strengthened. Again, the purpose of the question was to determine whether there are common outcomes across national and sectoral boundaries and which of these outcomes are shared by what percentage of respondents. This question was not mandatory.

Table 3 reflects that a large section of the respondents (43%, representing 48% of the countries and 80% of the economic sectors) want to see education, training, development and research in the profession improved. Most of these respondents want international certified or accredited training and education programs. The second most common strategy offered was that there should be a concerted public relations campaign to reach executives, HR personnel, clients, and other stakeholders to articulate the task and value of security risk intelligence analysis in the private sector.

A total of 37% of the respondents, which represent 43% of the countries and two-thirds of the economic sectors, feel that this type of intervention will address their previously stated challenge that people in and outside the organisation do not know what they are doing. Comments such as “getting buy-in outside the security department and getting power within the security department”, “helping decision-makers or clients who use analysis to understand more about the profession and what analysts do (and cannot do!)” and “it should be championed at C suite level as an enabler rather than a hindrance” reflected these suggestions.

The other identified themes reflect some of the previously identified challenges, specifically that HR practices should be improved so that the recruitment and retention problems are sufficiently addressed. Most of the 18% of the respondents, who represented nearly half of the economic sectors, suggested that HR practices be improved. They feel strongly that security risk analysis should not be seen as “a second career for the military/law enforcement, or something that people who cannot cut it as operators do… as our identity will be muddied and devalued”.

Table 3:

Suggested strategies to strengthen the professional identity of the security risk intelligence analyst profession: n=60

Themes identified	% of respondents whose answers included a code in the theme: *n*=60	% of countries whose answers included a code in the theme: *n*=21	% of economic sectors whose answers included a code in the theme: *n*=15
Improved and targeted training, education and research	43%	48%	80%
Improved articulation of identity and contribution within and across organisations, professional bodies and society	37%	43%	67%
Improved HR practices	18%	19%	47%
Enhance the role of professional bodies	10%	14%	33%
Self-awareness and ethical behaviour	10%	29%	27%

Suggestions to enhance professional bodies' role (offered by 10% of the respondents) included that these associations should provide certified career pathways and give recognition to experience and accomplishments, including success stories where analysts' work led to successful convictions or threat mitigation. The theme of self-awareness and ethical behaviour stressed the importance of analysts' commitment to ensure the highest ethical behaviour standards and provide reliable and credible professional advice. Other terms used by the respondents included "trustful", "taking ownership of their responsibilities", and being "transparent in their analysis methods".

4.6.7 The required skills to ensure that security risk intelligence analysis remain relevant in the future

An optional question was included in the survey, which prompted the participants to indicate which skills they think SRIA would need to remain relevant in the fast-changing private sector environment. A total of 52 respondents offered various opinions about the required skills in the face of the challenges they face and artificial intelligence developments that could replace analysts' media monitoring functions. The analysis of this specific question's results was done deductively, using the four broad future intelligence analysis skillsets identified by Hare and Coghill (2016) as categories or

themes (see Table 4). The most prevalent skill is that of "information management", which the researchers define as the analysts' ability to understand and interact with data tools & data analytics. Hare and Coghill (2016) state that

> "Tomorrow's cadre of analysts will need more explicit training or experience in method, reasoning, logic, and inference: a basket of skills that enable robust analytical structures to be spun from the tangled wool of messy problems and represented within the literal mind of a machine".

The 58% of the respondents, representing 47% of the 15 countries, but 86% of the 14 economic sectors, agreed with this typology and stated that analysts would need to be skilled in:

- Dark web exploitation
- Data visualisation and use of infographics
- Coding, data science, data ethics
- Using quantum computing power and creating real-time response algorithms to spot vulnerabilities

The second most prevalent required skills set is that of "collaboration", which relates to a better understanding of the decision-makers requirements *and* collaborating with peers to present the required information in tight deadlines in the right format. Half of the participants, but most of the countries represented in the answer set, agreed that collaboration and the skills that make collaboration happen would be crucial for future analysts. The emphasis was on the analyst's responsibility to understand his context and reach out to other stakeholders to understand their intelligence needs.

Statements such as "analysts need knowledge of individual private sector industries to understand better the threats posed to employees daily" and "to speak the business's language - it is the only way companies will maintain their in-house intelligence programs" were typical of the responses.

Table 4:

Suggested skills and attributes to strengthen the professional identity of a security risk intelligence analyst profession: n=52

Themes	% of respondents whose answers included a code in the theme: *n*=52	% of countries whose answers included a code in the theme: *n*=15	% of economic sectors whose answers included a code in the theme: *n*=14
Information management skills	58%	47%	86%
Collaborating skills	50%	67%	71%
Attributes	15%	47%	29%
Creative skills	10%	20%	36%
Thinking and reasoning skills	8%	20%	21%

This kind of immersion into the business would need "flexibility in various cultural environments", the "ability to adapt to changes quickly" and "expert adaptability such as being able to integrate with the other departments within a given business (e.g. R&D, manufacturing, supply chain, commercial, finance and so forth." One respondent eloquently states that "I think good analysts should broaden their experiences within their security shops and throughout their respective organisations."

The third most mentioned skill referred to attributes that respondents felt analysts should have and develop. The respondents offered flexibility, continuous learning, resiliency, adaptability, listening skills and resourcefulness. Fourthly, "creativity" was stated as a required skill, with comments such as "creative thinking for how to provide value (we are analysts before we are security professionals, so move outside the security box and focus on being someone who can answer questions" and "imagination and innovation in analysis and delivery" were offered. Lastly, "thinking and reasoning skills" were suggested by some respondents, but they generalised analytical thinking skills, without offering detailed descriptions of what they meant by this skill.

4.7 Discussion

In this study, collective professional identity has been defined as both the individual's sense of belonging to the professional group and the group's shared behaviour and values, perception or collective action. The survey's research objective was to determine whether such a shared collective professional identity exists among professionals who

conduct security risk intelligence analysis in the private sector. This international study is the first to explore the collective professional identity of an emerging profession in the private sector that contributes to protecting companies' employees, clients, their processes and products, against an array of traditional and hybrid threats.

As with any other exploratory study, the survey results are not definitive, mainly due to the unknown representativeness of the respondents (Babbie, 2015). However, the survey results provide sufficient evidence that the *respondents indeed share a collective professional identity even though they are from diverse national and organisational backgrounds*.

The demographic factors themselves provide a good indication of the potential strength of SRIA' professional identity. The demographic results concur with Alvesson (2001) that a high level of education (the majority of respondents have Masters degrees), status (68% are in supervisory positions, 69% belong to professional organisations, and 31% mentioned that they value self-esteem and external image the profession gives them), agreeable salary (only five of the 75 respondents complained about their salary) and exciting work tasks (half of the respondents enjoy the intellectually stimulating work) facilitate positive identity constructions.

A further indication that the sample size's collective professional identity is healthy is that the mean years of experience of the respondents are between 11 and 15 years. The majority have worked for the government in similar roles previously, consistent with the assertion (Jebril, 2008) that the professional stage exhibits the most solid phase of professional identity development. The study's international scope confirms Miscenko & Day's (2016) assertion that the growing globalization of occupations brings about standard practices allowing professionals to identify with an occupation that transcends national borders.

4.7.1 Sharing of individual belongingness to the profession

Therefore, the survey's objective was, first and foremost, to determine whether the first element of collective identity (the individual's sense of belonging) is present among the

participants. The fact that 74% of the participants *self-identify as SRIA*, who perceive themselves to be part of an emerging profession in security risk intelligence analysis on an international level, is a significant finding in this study. The analysis also confirmed that the respondents' self-identification with the profession is not dependent on social interaction (Ashforth & Mael, 1989), such as belonging to a professional organisation, even though most of the respondents belong to such organisations. Social interaction, networking, and sharing best practices would only strengthen the pre-existing sense of belonging and need for professional self-enhancement. It is not an indicator of or a prerequisite for a strong professional identity.

4.7.2 Shared professional behaviour or collective actions

The results indicate that the participants have similar viewpoints on most of the core elements of their professional identity, thereby indicating a collective or shared professional identity. These elements include their role and function, their self-perception, values and experiences.

i) A shared role and function that emulates meaningful work

Contrary to government intelligence analysis scholars' statements that the analysis function there still does not "know itself" and is not susceptible to a precise definition (Herbert, 2013; Kerbel, 2008), *this study showed that SRIA in the private sector generally agree with what their role and function is.*

The vast majority of the respondents (78%) stated that their main task is to provide forewarning to clients by identifying and analysing threats and risks through situational awareness. The function of **warning** is the universal fundamental task for intelligence analysts. The "forewarning" and "foreknowledge" roles also directly relate to the "emergent risks" aspect of enterprise risk management. A third of the respondents also stated that they provide actual security risk management advice to clients indicates that they have started to find a niche for their skills in the corporate world. It seems as though the security risk intelligence analysis profession is starting to come to its own in the private sector and increasingly do not need to "legitimise" themselves by

deliberately linking it with enterprise risk management to be seen as a credible partner to business success (Petersen, 2013).

The rhetoric used by the respondents to describe their role and function also have implications for their collective professional identity. The use of almost mythical words like “forewarning”, “anticipating and mitigating risks and threats”, “forecasting”, “making sense of the past and the present“, and “provide insight” concurs with Alvesson’s research (2001, 2011) that knowledge-intensive workers (such as consultants or in this case intelligence analysts) use rhetoric skills or symbolism to describe their claimed core product (knowledge), what they are doing (working with knowledge) and the results of that work and its meaning to clients. This rhetoric also strengthens their professional identity because it is seen as the essence of their trade, resulting in a mutually beneficial relationship where the more they use rhetoric, the stronger their professional identity becomes.

ii) A shared positive self-perception of the profession

The vast majority (75%) of the participants have a good perception of their profession and recommend the job to other people with the same interests and skills. This forms a good foundation for the formation and growth of the professional identity of this career group. Also, the participants have a similar idiosyncratic perception that they offer—according to them—something unique that no other profession does. Within the context of professional identity, it is irrelevant whether the function, role, or contribution to stakeholders is unique because no one else has a similar role. When individuals or groups construct their professional identity, they subjectively make sense of and articulate their perceived uniqueness or distinctiveness in their quest to find ways to contribute meaningfully to society (Wilkinson, Hislop, & Coupland, 2016).

The three equally important unique contributions identified in the study put the newly discovered professional identity on solid ground for further research. According to SRIA, their uniqueness lies in the fact that they:

- provide insights into threats to a business, economic sector, industry or national security;

- enable more informed decision-making by stakeholders and
- enable a safe working environment, risk reduction and loss prevention for companies that contribute to national economies.

Most of the respondents stated elements of all three themes in their answers and only differed in the organisational contexts they placed their perceived unique contributions. These unique professional contributions could be the primary marketing themes to future clients, colleagues in related professions and other stakeholders.

iii) Shared values

The shared values of integrity, honesty, and objectivity that most participants offer are typical of many professions and not unique to security risk intelligence analysis. If the survey has listed specific values and the participants ranked them, the results might have been clearer and more uniform. The evidence of Turner's self-categorisation theory is reflected in the fact that most participants self-categorised, associated or identified with a group whose values and ethics, whether explicit or perceived, are similar to theirs. The fact that respondents who do not work in security companies or who have to fend for themselves as entrepreneurs value their ethics, i.e. integrity, honesty, courage, learning and lawful, higher than the those working daily in a security-related environment, emphasises how they feel strongly about their ability to portray a particular type of personality and work ethic.

In emerging professions, like security risk intelligence analysis, there is often no specific or codified set of rules that could serve as a Statement of Values. Only one professional organisation, the Association for International Risk Intelligence Professionals (AIRIP), has a Code of Conduct (2015) for its members explicitly focused on the function and role of SRIA. Their values are very similar to those in the survey: loyalty, truthfulness, lawful, objectivity, honesty, professionalism, and responsibility. Statements like these official Codes of Conduct help define, reinforce and crystallise a shared sense of professional identity (O'Flaherty & Ulrich, 2016). Although professional membership is encouraged and assists in forming professional identity, it must be kept in mind that one does not need to be a member of a professional organisation to support the values it presents.

The person's self-identification and belongingness to the profession are more reliant on the values it represents than the membership of a professional organisation.

iv) Shared challenges

In what might seem contrarian, even the challenges that the survey participants faced could positively impact the formation and maintenance of the career group's professional identity. The fact that the respondents face various challenges, of which the most shared challenged (which 51% of the respondents shared) is that of their colleagues and clients not knowing what intelligence is and can do for them, is indicative of an emerging profession that has not yet marketed and established itself. It is also consistent with the notion that experienced professionals (as is the case with the participants) are generally satisfied with themselves and rely less upon others to form their professional self-image and conduct their work (Alves & Gazzola, 2011). This self-sufficiency and the "black box mentality" of corporate security (Crump, 2015) foster a secretive, ambiguous working environment in which analysts cannot convey what they are doing and how they are doing it. Unfortunately, this mentality and ineffective marketing will be the death knell for the profession in the commercial world beyond the security department. The public's unfamiliarity with the profession and the value it brings to companies and society as a whole need to be countered by increased visibility. This visibility should improve the profession's organisational environment, networks and ultimately, how others perceive it.

4.7.3 Professional identity elements that are not shared

There are two elements that the participants do no share: *a similar job title* and *the benefits they derive from being in the profession*. These elements are not as crucial to the formation and maintenance of professional identity as self-identification, self-perception and other's perception. The lack of a similar job title could be due to the lack of support and cooperation with HR has been identified as one of the significant organisational challenges that the respondents face. The third reason might be that due to the complex nature of the work done by respondents situated in different functional areas within the organisation, that would impact their job title.

This analysis confirms what Petersen (2013) calls the "hybridity" of people in corporate security, who are neither entirely situated in the field of security nor the field of business, or as the results of the survey suggest, execute different roles within corporate security. Unfortunately, the survey did not attempt to gather data on the other roles the respondents would fulfil in corporate security, which could have given the context of the other roles and that of a security risk intelligence analyst they fulfil.

The complexity and variety of intelligence focus areas or topics that SRIA in the private sector research and advise on is congruent with Peterson's (2013) assertion that corporate security has widened to include risks and threats that have been the domain of national security to make the "entire society" more resilient and resistant to all kinds of threats. It is not known whether the absence of a shared job title like "teacher", "doctor", "advocate", and the like has an impact on the strength of the professional identity of SRIA. However, it is evident from previous research that similar job titles make it easier to self-identify or dis-identify as the name embodies the role that the person or group is performing and assist with external marketing (Neary, 2014). The fluidity and complexity of the functions that the participants fulfil might make it nearly impossible to standardise a job title as that would then 'limit" the understanding of potential clients on what this profession can offer. Further research is necessary to determine whether the target group think a standardised job title could provide organisational and external currency, thereby strengthening their professional identity.

The analysis that the respondents *do not share common benefits* that they derive from being in the security risk intelligence analysis profession is understandable and does not impact on the main finding that they have a shared professional identity. Each participant has their circumstances and motivations for becoming and remaining in the profession. The only benefit mentioned by the majority (51%) participants is the intellectually stimulating nature of the work. This finding can prove useful for recruitment and retention purposes as people who are naturally inclined to be inquisitive, love reading, writing, learning and passionate to "be-in-the-know" might have a better chance of job satisfaction. The idiosyncratic nature of job satisfaction and

how it impacts professional identity will be addressed in Study 2 during the interviews of the ten individual SRIA.

4.8 Limitations

The exploratory research of the perceptions of the target group, whose existence and extent was unknown, is always problematic as it clouds the research's validity. Therefore, the main limitation of the study was the fact that the sample may not be representative. Also, the subjective nature of self-perception could be time and context-based, thereby increasing the research topic's ambiguity further. One could take the approach that the survey merely reflected a “snapshot” of the conscious process of self-categorisation and the respondents' self-identity at that specific time. In that case, the value of the research becomes more visible.

Another limitation of the data analysis was that the researcher had to caution against the temptation to compare countries due to the data's heterogeneity. Often, the researcher was tempted to compare a single respondent's data from country X to the 33 from country Y but refrained because the outcome would not be valid as it was not known whether the respondent pool is a typical representation of the target population in those countries. The researcher aimed to interpret different combinations of demographic variables to understand the nuances of the participants’ collective professional identity. However, as it would not withstand the representativity test, cursory remarks were made to indicate possible interesting hypotheses that could be tested in further research.

4.9 Conclusion

The quantitative study's objective has been met in as far it has empirically proved that 75 professionals from 27 countries self-identify as SRIA and have a shared collective professional identity. Despite being a new or emergent profession, most participants exhibited that they individually have a sense of belonging to the professional group and that the whole group shared a common understanding of their role and function, their self-perception about the profession, as well as their values and experiences.

They perceive their professional role as meaningful when they provide critical forewarning and situational awareness about the company's threats and risks. They see themselves as a valuable partner in protecting the private sector's interests, including their employees, clients, processes and products or services. Their main shared frustration or professional challenge is that people in their own organisation, and sometimes clients, do not understand their function and what value they bring to the management of a company's operational risk.

However, their collective professional identity is vulnerable because they do not share a common job title and that outsiders do not perceive them favourable enough to be considered critical to business' success. These challenges could be overcome by measured marketing and influencing efforts to the different stakeholders. These should include human resources personnel, universities and the broader security and corporate risk community through awareness efforts that should highlight the function, value and skills that the profession offer in a world that has become increasingly dangerous for the private sector to operate in.

Chapter 5

Study 2: An interpretative phenomenological analysis of the lived professional experience of SRIA in the private sector

5.1 Introduction

Where the survey aimed to determine the collective professional identity of SRIA in the private sector, the qualitative part of the mixed methods research design aimed to answer the second research question, namely, what is the individual SRIA's professional identity? The way in which the study attempted to answer the research question was to focus on their lived experience by giving them a voice to share their search for professional meaningfulness and their sense-making in the face of professional challenges and opportunities. Interpretative Phenomenological Analysis (IPA) was deemed to be the most appropriate qualitative research method to explore the study's third research objective of understanding how individual SRIA in the private sector experience their profession in an individual or idiographic manner.

The main objective of IPA is to understand what personal and social experiences mean to the people who experience them and then analyse how participants make sense of and give meaning to their lived experience (Smith et al., 2009). This chapter will detail the IPA research methodology, the process that was followed in the analysis of the interviews with the participants, present the findings and discuss the results relating to literature, deal with the study's shortcomings and touch on possible avenues for further research.

5.2 Research method

5.2.1 The interpretative phenomenological analysis (IPA) approach

IPA is a relatively new research methodology introduced by Jonathan Smith in the 1990s in the UK's psychology field as part of the family of phenomenological approaches to the psychology of experience in health, clinical and counselling psychology (Eatough &

Smith, 2017). IPA has two primary aims: to look in detail at how someone makes sense of life experience and to give a detailed interpretation of the account to understand the experience (Tuffour, 2017).

IPA is a useful method in social science where researchers give voice to the participants' experiences, followed by sufficient and credible interpretation of their narratives. The IPA methodology has been applied in various disciplines other than the original psychology. With specific reference to the study of professional identity in different professional contexts, IPA has been used in education (e.g. Wood, Goodall, & Farmer, 2016), organisational studies (e.g. Gill, 2015), health studies (e.g. Sylvia, 2018), occupational therapy (e.g. Warren, 2014), psychology or counselling (e.g. Idowu, 2017; Verling, 2014) and even working environments like the Army (Dynes, 2014; Topp, 2015), security industry contractors in Iraq (Messenger, Farquharson, Stallworthy, Cawkill, & Greenberg, 2012) and the National Aeronautics and Space Administration in the US (Becker, 2020). The IPA methodology has not yet been used in security risk management or intelligence disciplines, which adds to the current study's value to understand the personal experiences of professionals in the private sector.

5.2.2 Rationale for using IPA as a preferred qualitative research method

The main reasons why IPA has been chosen as the preferred qualitative research methodology were fourfold. Firstly, IPA has been found useful by other researchers when exploring a new phenomenon in which people whose lived experiences have not yet been investigated, as is the case with this study. This exploratory approach provides useful cues for understanding the phenomena and give direction for further research. Secondly, as seen from the studies above, IPA has been proven to be a suitable approach for investigating individual identity construction and their lived experience after Smith pointed researchers to this possibility (2009). Thirdly, IPA offered an accessible, systematic methodology for the researcher (who has a little psychological background) as it provides the theoretical framework (phenomenology), the types of questions to ask, the sampling strategy (a small, homogenous number of participants), the data

collection method (semi- or unstructured interviews) as well as the analytical procedures to be followed.

Lastly, IPA embraces the insider perspective by accommodating the researcher's own experience as a security risk intelligence analyst in the private and government sector. Alase (2017) states that for the participants' lived experience to make sense interpretively, the interpreter must have a "true and deeper understanding" of those lived experience by putting oneself in the shoes of the participants. IPA literature provides practical guidance on managing one's own biases and preconceptions in the interpretation process, mostly by using a reflexive journal and applying various interpretation strategies. The researcher will comment on the reflexive journey throughout the study later in this chapter.

5.2.3 IPA theoretical foundations

IPA relies on three fundamental theoretical underpinnings to examine the way people make sense of their experiences, namely phenomenology, hermeneutics and ideography. The following discussion is not exhaustive and only touches on the most relevant constructs as it applies to IPA.

i) Phenomenology

Phenomenology (Greek: to show itself or bring to light) is a well-known philosophical approach to studying human experience in all of its aspects, but specifically to those things that make up our lived world and the meaning we give to it. IPA does not prefer a specific school of thought in phenomenology but sees the different emphases of Husserl, Heidegger, Melreau-Ponty and Sartre as complementary to create a "mature, multi-faceted and holistic phenomenology" (Smith et al., 2009).

Adopting Husserl's "phenomenological attitude", which involves one's conscious focus or reflection on the thoughts, values, goals or means involved in a specific experience, IPA established itself as a systematic approach that reflects on the actual activity as well as the mental and affective responses to that activity. Furthermore, IPA concurs with the critical importance of the interpretation of people's meaning-making in

phenomenology by adopting Heidegger's construct of *"Dasein"* or "there-being" in which he explains that a person is always in a world of objects, relationships and language and that this being-in is always relying on perspective, is temporal and in relation to something else, therefor must be interpreted as such. Smith et al. also support Merleau-Ponty's view that the self's embodiment subjectively shapes one's experience, while Sartre's layered analysis of experience is contextualised in the presence and absence of relationships with other people resonates in IPA's purposeful layered interpretative analytical process. In summary, Smith et al. (2009, p.27) state that

> "… through the work of all of these writers, we have come to see that the complex understanding of 'experience' invokes a lived process, an unfurling of perspectives and meanings, which are unique to the person's embodied and situated relationship to the world."

ii) Hermeneutics

IPA is also interpretative, meaning that it goes beyond the descriptive to explain and interpret individuals' lived experiences. Interpretative phenomenology is based on hermeneutics, which is the theory of interpretation or meaning that can be traced to Greek philosophy and later biblical exegesis. It aims to understand the methods and purposes of the interpretation process, including whether it is possible to uncover the intentions of an author or speaker and the relation between the context of the author and the interpreter (Tomkins & Eatough, 2018).

Following Schleiermacher, IPA posits that the interpreter can, through a range of skills and intuition, conduct a detailed, comprehensive, holistic analysis that can understand the participant better than he understands himself, or at least the explicit claims of the participant (Smith et al., 2009). IPA can offer a perspective that the participant alone cannot. The IPA researcher's added value is the systemic and detailed analysis of a text, brought about by having oversight from a more extensive data set and access to other theories.

The hermeneutic circle is used to depict the dynamic relationship between the part and the whole on a series of levels in which one needs to look at the whole to understand one part, while you need to look at the parts to understand the whole. This dynamic and

active interpreting role of the researcher gave rise to IPA's double hermeneutic circle or dual interpretation process in which the researcher not only sees experience at face value but also as a whole while making sense (Pietkiewicz & Smith, 2014). In this process (see Figure 14 below), the research participant makes sense of his own experience (sense-making), while the researcher makes sense of the participant's sense-making and gives it meaning (meaning-making). In this iterative and inductive interpretative analysis process, the researcher employs various interpretation strategies (the outer layer of the double hermeneutic circle) to assist in her meaning-making and ensure multi-layered and rich interpretation. These interpretation strategies give the researcher entry to the meaning-making process while providing different perspectives on the text's part-whole coherence (Smith et al., 2009).

As IPA's main objective is to understand what an experience is like from the participant's perspective by putting oneself in the shoes of the participant, the primary interpretation strategy follows Ricoeur's hermeneutics of empathy which aims to produce a rich experiential understanding of the phenomenon and remain close to the participants' sensemaking (Eatough & Smith, 2017). Most of the IPA literature employs the

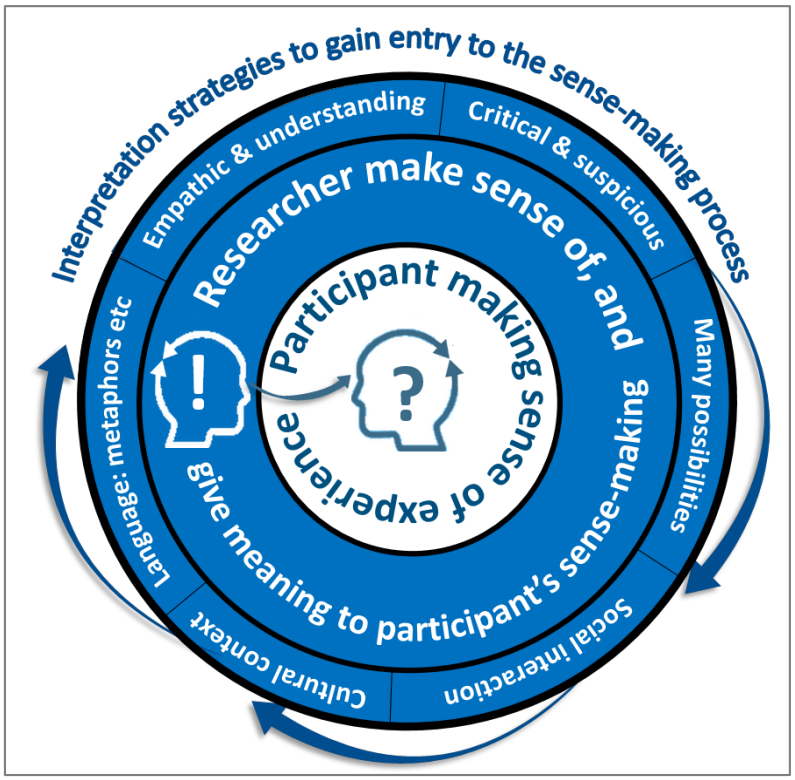


Figure 14: The double hermeneutic circle with interpretation strategies for the researcher

empathetic interpretation strategy to enter the sensemaking process by focusing on their experiences (Larkin, Watts, & Clifton, 2006) as well as interpreting the language used like metaphors, symbols and temporal construction of the experience, including the use of present tense vs past tense (Pietkiewicz & Smith, 2014).

However, the researcher also needed to put aside what she believed at face value and looked for a deeper meaning that the participants might be unwilling or unable to do themselves by asking critical questions about intentions, subtle meanings, undisclosed feelings or agendas, and nuances in the participant's sense-making, after Ricoeur's hermeneutics of suspicion (Shinebourne, 2011). IPA does not take this critical approach to include psychoanalysis or psychological theory, as Smith et al. (2009) deemed this as "reading something into the text" that the participant did not offer. The researcher had to be sensitive to guard against superimposing her own experience or theories on the participant's text and sensemaking by frequently verifying her interpretation against the entire text and the iterative process of analysis—the typical hermeneutic circle. When one wants to bring theory to assist in the analysis, it must be clear that this is the researcher's subjective interpretation and not the participant's text. Therefore, the researcher was acutely aware that there are different interpretation possibilities and that her interpretation was merely a subjective analysis or a snapshot of her interpretation in a specific time and place and that another researcher might interpret the participant's experience differently.

iii) Ideographic

IPA is "committed to the detailed examination of the particular case… and wants to know in detail what the experience for *this* person is like, what sense *this* particular person is making of what is happening to them (Smith et al., 2009). The ideographic philosophical foundation of IPA has two dimensions: firstly, its commitment to the particular detail and the depth of analysis and secondly, its commitment to understanding how specific phenomena have been understood from the perspective of particular people in a particular context. This idiographic focus on the individual experience makes IPA useful to explore the complexities, richness and thickness of an unresearched topic such as the professional identity of SRIA in the private sector.

Therefore, the sample size is relatively small and reasonable homogenous so that convergent themes, as well as divergent experiences, could be found amidst the individual participants.

5.2.4 The IPA Process

Smith et al. (2009) propose a six-step process that provides guidelines for the novice researcher to conduct an IPA study. These guidelines make the analysis process more manageable, although the researcher needs to understand that it is iterative and dynamic and not necessarily linear. In this vein, the researcher customised the IPA process (Figure 15) for this study as a two-phased, seven-step process based on or built on the three theoretical foundations of IPA discussed above.

In the first phase, consisting of 5 steps, the researcher started with Step 1, in which the transcript and recording were read and re-read to obtain an overall perspective of the interview. In Step 2, the researcher did some initial noting to produce a comprehensive and detailed set of notes and descriptive, linguistic and conceptual comments on the data. In Step 3, the researcher developed emergent themes by applying the hermeneutic circle to determine what might be a crucial reflection of the participant's sense-making and the researcher's understanding. In Step 4, the researcher searched for connections across the emergent themes to produce a structure of the participant's account's most important and interesting aspects. In Step 5, the researcher moved to the next participant's interview, deliberately bracketing the previous case and treating the new participant on their terms. These five steps are then repeated for each participant.

After all the separate cases have been analysed, the researcher moved into the second phase in Step 6, where she looked for patterns across all the cases, recurring or convergent themes, contrasting or divergent themes. Finally, in Step 7 (which the researcher has added to Smith et al.'s six-step process as they do not acknowledge this as a further step), the findings were interpreted across the cases and written up. The researcher had to apply double hermeneutics in five of the seven steps, thereby ensuring that the interpretation was rich and reflected the researcher's various levels of

analysis in the sensemaking and meaning-making process. The detailed description of the process followed in the study is discussed in the data management and analysis process description.

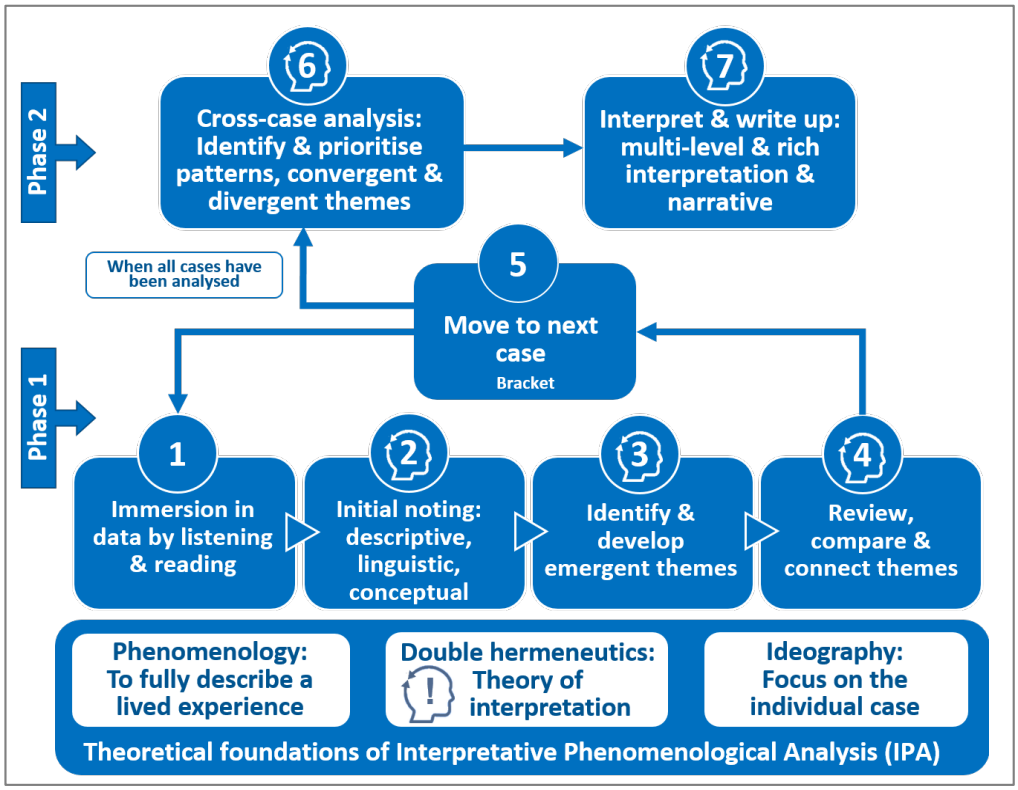


Figure 15: The 7-Step Interpretative Phenomenological Analysis process with its three theoretical foundations followed in this study (based on Smith et al 2006)

5.3 Ethical considerations

The Ethics Committee of the University of Portsmouth approved the interview schedule, information sheets and consent forms, and the data processing and retention processes (see Appendix D1). There were four risks identified that needed to be addressed in the study. Firstly, the confidentiality of the identity of the participants could be breached. To minimise this risk, all identifying information like the interviewees' names and their employers were removed to ensure anonymity. All transcripts were shared with the interviewees to ensure that the transcript was a true reflection of the interview and that any identifiers have been removed. Only one interviewee had to have the transcription of his interview approved by his employer. Secondly, the confidentiality of the information had to be guaranteed by using a password-protected computer that is only

accessible to the researcher and storing the data on this protected computer and a secure devoted server administered by the University of Portsmouth.

The third risk was that the participants' emotional and psychological wellbeing could be affected by sharing experiences in the interview. Participants were informed that they had a right not to answer a question if they feel uncomfortable with it and that they can withdraw from the study at any time. None of the interviewees withdrew during or after the interviews. The researcher found that most of the participants enjoyed talking about their personal, professional experiences, many of them for the first time. Two participants remarked that the interview allowed them to reflect and gain perspective on many aspects of their work-life that they never considered before.

The qualitative study's primary ethical consideration was the possible impact of the researcher's personal experience to define her professional identity when she moved to the private sector as an intelligence analyst. Although this is ideal for an IPA research study as it provides valuable insider insight, it is necessary to manage possible ethical challenges. The researcher could not allow her knowledge, experience, and preconceptions to influence the interpretation and analysis of the interviews and the data and the familiarity with terminology that might have influenced the conduct and analysis. The chances that both the participants and the researcher made assumptions that could have led to misunderstandings and misinterpretations of experiences could also not be excluded. The researcher was aware that her professional relationship with four of the ten interviewees could have influenced the interview dynamics. It was, however, found that the familiarity resulted in more personal reflection and overt sensemaking that was not necessarily found with the other interviewees.

In her effort to be an ethical and moral responsible researcher (Johnsson, Eriksson, Helgesson, & Hansson, 2014), the researcher acknowledged that she could manipulate or direct interviews and interpret participants' experience. She realised that she had a responsibility towards science, the university and the participants to manage this "power" effectively by maintaining a reflexive or self-aware attitude throughout the study. A reflexive journal (see Appendix D2) assisted the researcher to document her

thoughts throughout the study. Interaction with her supervisors and other researchers also helped the researcher remain conscious of ethical conflicts in data interpretation.

5.4 Research procedure

5.4.1 Interview schedule design

IPA studies are inductive and focus on the ideographic experiences of a small target group. This study's questions aimed to obtain rich and detailed descriptions of how individuals experience and make sense of their professional identity in their professional lives. The qualitative study's main research question is, "how do SRIA in the private sector experience their profession, and how does this impact their identity?" Interview questions were formulated to reflect the study's research questions (see Appendix D3). Questions focused on people's experiences, perceptions and views on the phenomenon of professional identity (Smith et al., 2009) and included the following:

- What does being a security risk intelligence analyst mean to you personally? What makes this career different from any other career?
- In your experience, what are the biggest challenges you experience/d as a Security Risk Intelligence Analyst? How did you overcome/are you overcoming these challenges?
- Did you ever feel you had a professional identity crisis as a security risk intelligence analyst? What happened, and how did you deal with the experience?
- In your experience, how do other people perceive you as a Security Risk Intelligence Analyst? How do you feel about that?

The interview schedule started with demographic details to set the stage for the interview, give context in terms of the participant's professional experience, and lead the discussion into more intimate details about their lives. The questions also had prompts should the interviewees struggle to verbalise or share their experience upfront. The questions were sufficient to determine whether the interviewees perceive themselves to make a unique contribution to the organisations they work for and the

broader society (meaning-making of their professional purpose) and how they make sense of challenges and opportunities in their professional lives (sense-making).

5.4.2 Recruitment

The sampling strategy for the semi-structured interviews was purposive as participants emanated from the survey and self-identified as SRIA. The survey ended with an optional email link to the researcher if participants were willing to be interviewed in the second study. The ten participants were provided with consent forms for the interviews (see Appendix D4). Four participants were from the US, two from South Africa, one from Canada, the UK, Germany and a South African working in the US).

This homogeneous group (concerning their profession) conform to IPA requirements of selecting a defined group for whom the research problem has relevance and personal significance (Pietkiewicz & Smith, 2012). The only criteria for the interviewees were that they should have had at least three years of practical experience in the private sector to exclude newcomers who might not be able to relate to the research objectives. They had sufficient experience to generate an in-depth exploration of the lived experience of their professional identities as security risk intelligence analyst in the private sector.

5.4.3 Data collection

The semi-structured interviews were conducted using the Skype and BlueJeans internet communication applications preferred by the participants, or in-person in February and April 2019 and March 2020. The last two interviews took place a year later than the others in consultation with the researcher's supervisor to extend the participant pool and geographical representation. Before the interviews commenced, the interviewees were reminded of the study's purpose, their anonymity, the confidentiality of the information they shared, and the right to withdraw, as reflected in the consent forms they signed. They agreed that the interviews can be recorded for transcription purposes and reiterated their willingness to participate in the study.

The interviews ranged from 35 to 107 minutes in duration. The researcher transcribed a total of 695 minutes with NVivo12 Transcription in February and March 2020. The

transcriptions amounted to 112 A4 MSWord pages with a 53,387-word count. The interviews (see Annexure D5) could roughly be divided into three major parts: the demographic narrative of who they are and what their work entails, their narrative about their lived, personal experience in the profession, and thirdly a segment on what they think can be done to strengthen the profession. The interviews and transcripts were stored according to the agreed data storage prescriptions of the University of Portsmouth on a password-protected computer of the researcher and the University's cloud server.

5.4.4 Data management and analysis

The researcher used an amended template for the transcript analysis proposed by Smith et al. (2009) by designing an MS Excel workbook in landscape format and dividing the page into five columns. MS Excel was more comfortable to use as a line-by-line analysis of the data facilitated the sorting and filtering of data and easier identification of themes and sub-themes. Columns could be hidden and unhidden, themes filtered and grouped and searched more effectively for the "gems" as insights deepened, and the process became more streamlined and effective.

The IPA method of data analysis discussed above was useful and helped the researcher maintain focus throughout the analysis process. The two main research questions were used as parameters and compass for the analysis and interpretation of the data. It proved easy to go astray with an interesting diversion that does not directly relate to the study. Each interview was analysed separately on a case-by-case basis on separate spreadsheets.

The far left column A was used to number the transcript lines (i.e. E23 for line 23 of Emma's interview), the column B for those parts of the transcript that were relevant for the analysis (pure biographical elements were removed in the sheet as it is reflected in the interviewee details hereunder), the third column C was used for Step 2 of the process - the initial notes and comments on the descriptive, linguistic and conceptual elements of the transcripts after each was read, and re-read at least four times (in

different colours). Interesting or useful sections or "gems" that could be used in the write-up of the analysis were identified and bolded in the text in Column B.

In Step 3 of the process, the transcript column was hidden. The comments in column C were analysed and abstracted as a further interpretative process by identifying and developing emerging themes and then put in column D. In step 4 of the process; these emergent themes were then filtered, similar themes grouped and further abstracted, some themes subsumed under more robust themes, others elevated in importance and others contextualised in Column E as "cluster" themes.

However, as the researcher analysed the next transcript, it became clear that most of the "cluster" themes in Column E might be similar. An alternative strategy, proposed by Willig (2013), was then followed whereby the original list of final themes for the first interview was used to code the other interviews, adding or elaborating on the themes as the process evolved. A separate Excel workbook was created for sheets for each of the identified superordinate themes, in which the matching subthemes were listed with the line number of the relevant subtheme, with the researcher comments and parts of the transcript for context, sometimes "gems" that could be used in the write-up of the analysis. In this strategy, it was prudent that the researcher followed the hermeneutic process. As her insight into themes grew, she went back to earlier transcripts to see whether a newly identified theme appeared in previous transcripts that she might have missed (Figure 16).

B	C	D	E
Original transcript	**Comments descriptive linguistic conceptual**	**Emergent themes**	**Cluster themes**
I want to branch out from what I'm currently doing. I've done analysis for over 15 years now. Now I want to go in to something new to do with investigations because I don't have investigation background.	Bored with this type of work. Branching out, means growing, as with a tree. She does not want to stagnate, Current work is not sufficiently enriching,	She feels stifled and needs to have space to grow and learn new things.	Confidence in cognitive abilities, skills and ability to stretch/grow
The reason why I registered with the ACFE is that I want to move into that space because I see it is more challenging than my current space.	Does not want to leave the current job without leaving a legacy - she wants to feel that she has achieved something, and that is a changed behaviour of the operational people who are now filing more complete investigation reports	She will change career - needs to be challenging	Confidence in cognitive abilities, skills and ability to stretch/grow

Figure 16: Screenshot of the IPA Excel sheet used for analysing Emma's transcript, with the cluster theme column filtered to reflect the provisional cluster theme of "Confidence in cognitive abilities, skills and ability to stretch and grow".

In Phase 2 of the IPA process (Figure 17), step 6 required that the researcher seek relationships between the different themes by identifying convergent and divergent

patterns in the themes and cluster them accordingly. When themes did not fit well with the emerging structure of themes, they were subsumed in other themes if they supported or strengthened that theme, or else were discarded if they did not fit well with the emerging paired themes and their arguments or basis was weak (Pietkiewicz & Smith, 2014). In the end, this resulted in an extensive list of subthemes under each superordinate theme, which then again went through the process of interpretation, abstraction and merging so that between three and five final subthemes under each superordinate theme were identified.

In step 7, the themes were analysed and explained with extracts or vignettes from the participants in this chapter's Results section. This step aims to detail the researcher's interpretations while retaining the emic voice of the participants' experience. Lastly, the researcher related the identified themes and the interpretations of existing literature in the Discussion section of the chapter and discussed the implications of the study, its limitations and possible future applications.

Superordinate theme 1: Purposeful professional self				
Sub ordinate themes	Points	Ideas/comments	Lines	Transcript
Self-concept	Traits	Humbleness and working in the engine room (support role) is important for him	A38	And I think I think if you can be humble enough it can be very satisfying.
Self-concept	Traits	Humbleness and working in the engine room (support role) is important for him	A40	And you know, it's really hard work we're doing. And it's hard trying to stay on top of things, if you can persevere through the end result whether that's a good case you resolved or you've influenced a business decision.

Figure 17: Screenshot of the final spreadsheet for the superordinate theme Purposeful Professional Self with the identified subordinate theme of Multi-faceted Professional Self-concept, with the identifier point "Traits", the researcher's comments and the transcript lines. The different columns could be easily filtered for analysis.

5.4.5 Interviewee details

The ten participants' demographic details and their working contexts were analysed as a precursor for analysing the interviews (see Table 5). The interviewees' average age is 45 years, with an average of 7.3 years of experience in the private sector. Eight of the ten interviewees were previously employed in the government sector in similar roles where they functioned as intelligence analysts. These eight participants worked an average of 12 years in the government before moving to the private sector. Only two

participants work for employers whose primary business is to deliver research or consulting services in security risk. The other eight participants work in security departments for organisations that provide services and products ranging from pharmaceuticals, beverages, telecoms, university and commercial banks and financial regulators. Half of the interviewees (5) work in small teams of between two and five, while the other five execute their function as the only person responsible for that role in the organisation. Four have Bachelor's degrees, two have Honours degrees, and the remaining four have Masters degrees, all in the Social Sciences.

Andy (A)

Andy is a 38-year-old male senior security analyst working at a pharmaceutical company in the US. He served as an intelligence analyst in the military for ten years and has worked in the private sector in the same capacity for the last six years. He is responsible for a wide range of functions, including investigation support, insider threats, physical security threat assessments, supply chain risk intelligence, and political and geostrategic risk assessments. He works in a small team that contracts in security risk consultancy firms to provide general assessments that the team then customises for internal consumption. He is a member of the Association for International Risk Intelligence Professionals (AIRIP).

Ben (B)

Ben is a 54-year-old male cybersecurity intelligence analyst and manager at a major research university in the US. He is responsible for analysing the threats to the university's IT system. Ben is the manager for cybersecurity and does the occasional cyber forensic investigation as well. He has fulfilled this specific role for the last nine years. Ben was a management consultant before this position and is a member of various professional organisations in the IT Security, cyber and intelligence domains. He is currently busy with a Masters in Intelligence Studies.

Table 5:

Information on the participants of Study 2

	Andy (A)	Ben (B)	Celia (C)	Dave (D)	Emma (E)	Josh (J)	Kate (K)	Lynn (L)	Tina (T)	Vic (V)
Age	38	54	64	50	47	30	34	54	38	37
Gender	M	M	F	M	F	M	F	F	F	M
Nationality	US	US	US	DE	ZA	UK	US	ZA	ZA	CA
Exp in role in private sector	6 years	9 years	10 years	20 years	3 years	3 years	3 years	8 years	4 years	7 years
Highest degree	B. degree	M. degree	B. degree	B. degree	Hons degree	M. degree	B. degree	M. degree	M. degree	Hons degree
Similar role in govmnt	10 years	No	30 years	No	12 years	7 years	12 years	16 years	5 years	6 years
Years work experience	16 years	30 years	40 years	25 years	15 years	10 years	15 years	30 years	15 years	13 years
Employer	Pharmaceutical	University	Consultant	Financial regulator	Commercial Bank	Telecom company	Beverages company	NGO/ Thinktank	Financial regulator	Financial industry
Member of prof org	Yes	Yes	No	No	Yes	No	Yes	No	No	No
Connect w other SRIAs	Yes (external)	Yes (external)	Yes (External)	Yes (External)	No	Yes (External)	Yes (External)	Yes (Internal)	Yes, both	Yes (external)
Date of interview	28 Feb 2019	22 Feb 2019	12 Feb 2019	25 March 2020	21 Feb 2019	25 Apr 2019	23 Feb 2019	25 March 2020	21 Feb 2019	25 Apr 2019
Transcript words	7965	4921	5580	3415	3211	5663	6440	2101	3916	10175
Length of interview (min)	107	79	64	48	43	79	76	20	47	102

**The names have been changed to ensure confidentiality*

Celia (C)

Celia is a 64-year-old female former analyst and manager in the US's intelligence community with 30 years of experience. She has been in the private sector for the last ten years. She worked in a management consulting firm before moving to a bespoke security risk analysis firm that provides advice to Fortune 500 companies. She does not belong to any professional organisations but is active in the profession and is often invited to speak at conferences. She serves on a few boards of organisations that promote national security, social sciences and intelligence analysis and mentor younger women in the intelligence community.

Dave (D)

Dave is a security risk analyst at a major European financial regulatory institution in Germany. He has an engineering degree and did electronic engineering and security

installations before moving to his current employer, where he has been for the last 20 years. Dave was one of the first people recruited to start a security risk management unit. He has a wide variety of skills and experience due to this, including doing threat assessments for VIP protection, ensuring secure building designs, and monitoring major political events and socio-economic trends. His current role is to understand and communicate the threat to the organisation in a multi-dimensional manner as the start of the security risk management function and any other role the organisation might assign to him. He does not belong to any professional organisation as he does not see the need "to sell himself".

Emma (E)

Emma is a 47-year-old female who has worked at one of South Africa's major commercial banks for the last three years as a crime analyst on serious and violent crime against the bank, i.e. armed robbery, cash in transit (CIT) attacks, ATM bombings and other physical threats against employees and clients. She has a post-graduate degree in criminology and worked as a lecturer at a local university and a financial crime analyst in the regulatory sector before moving to her current position. She is a member of the Association for Certified Fraud Examiners (ACFE) and wants to become a certified fraud examiner in the absence of similar certification in intelligence or crime analysis and improve her employment opportunities.

Josh (J)

Josh is a 30-year-old male security risk analyst in the telecoms industry in the UK. He has degrees in international politics and a master's degree in philosophy and served in law enforcement as an analyst dealing with terrorism and serious economic crime for five years. Three years ago, he moved to the financial sector, where he was an intelligence analyst dealing with threat assessment to the sector. He moved to his current position, where he provides cyber threat analysis a year ago. He is not a member of a professional organisation.

Kate (K)

Kate is a 34-year-old female analyst at a major beverage company in the US. She has a bachelor's degree in history and Russian and served in the US intelligence community for 12 years. She has been a senior risk intelligence analyst with her current employer for three years. Her team of five analysts was responsible for a wide range of security risk and opportunity assessments in countries where the company has business interests. They focus more on broader strategic and geopolitical risks and opportunities than tactical physical security threats. Their clients within the company include Supply chain management, Operations, finance, and Human Resources, all of which need information and advice on anything from modern slavery, geo-political events, currency and commodity futures, social impact, and corporate responsibility issues. Kate is a member of the Association for International Risk Intelligence Professionals (AIRIP).

Lynn (L)

Lynn is a 54 year old South African working in the US at an NGO/think tank that provides analysis and advice to various companies and other NGO's regarding security, risk and governance issues. She has a master's degree, previously worked in the South African Defence Force as an analyst and has worked for the last nine years in the private sector analysing threats in the maritime environment. She does field research, runs a database on her desk and produces various analytical reports on maritime crime. She is not a member of a professional organisation.

Tina (T)

Tina is a 38-year-old South African security risk analyst in the financial regulatory sector. She has a Master's degree in Applied Intelligence from a US university. She was previously a researcher in the energy sector, where she mainly researched Africa's energy market. She worked as an intelligence analyst in her current employer's security management department for three years before becoming the unit manager when the post became vacant. She has a team of 4 analysts that provides analytical products and services to various internal stakeholders, including the physical security team, the VIP protectors, the supply chain management department, and departments requesting due

diligence investigations into people and companies. She was a member of the Association for International Risk Intelligence Professionals (AIRIP) but cancelled her membership as the distance meant that she could not attend any meetings or events.

Vic (V)

Vic is a 37-year-old male working in the Canadian financial regulatory sector as a senior intelligence officer. He has a post-graduate degree in political science and international relations. Vic has 13 years of experience in intelligence analysis, seven in the Canadian armed forces and law enforcement and six years in the private sector. In his current position, he is responsible for a wide range of functions, of which threat intelligence is just one. He also executes the entire security risk management function, including building vulnerability and risk assessments and security countermeasure implementation. He is a member of three professional organisations as he values learning opportunities and networking.

5.5 Results

The following section will detail the findings of the IPA process of the lived experiences of the ten participants of being a Security Risk Intelligence Analyst in the private sector. As seen from the demographic analysis, the participants all have a unique background and are from different countries.

The researcher was doubtful whether there would be sufficient shared perspectives and experiences among the participants' different experiences and professional journeys but was pleasantly surprised at the findings. The analysis process discussed resulted in three superordinate themes that emerged from the transcripts:

1. Purposeful Professional Self
2. Connectedness to Professional Others
3. Enacting Professional Identity in the Workplace

Figure 18 provides an overview of the identified superordinate and subordinate themes. Each of the themes will be discussed narratively by illustrating the themes shared across the data with quotes from participants divulging their unique perspectives.

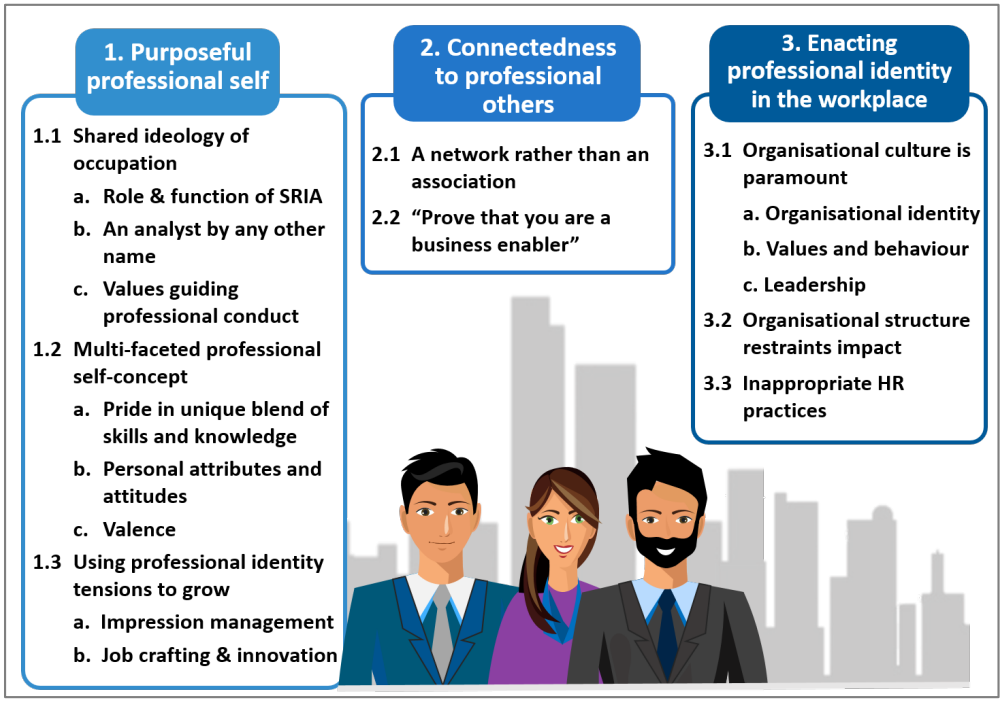


Figure 18: Identified superordinate and subordinate themes

5.5.1 Superordinate theme 1: Purposeful Professional Self

The superordinate theme *Purposeful Professional Self* refers to the participants' self-perception of their profession and their lived experience of their journey to meaningful work as a security risk intelligence analyst in the private sector. This theme focus on the intimate, personal and reflective experiences of their professional life that the participants shared during the interviews. All the participants indicated that they have never had the opportunity to think about how they feel about their profession and what they bring to the table that is truly unique and contributes to the organisation and the wider society's well-being. The three subthemes are depicted in Figure 19.

The first subordinate theme is *Shared Ideology of Occupation*, which refers to the shared understanding of the meaning and purpose of the occupation and their experience on the significance of job titles and values for executing the SRIA role; the second is *Multi-faceted Professional Self-concept,* which reflects the foundation of their professional identity, which is constituted by their 1) skills and knowledge they use in the execution of the SRIA role, 2) their characteristics or traits that they use that lead to their perceived success within the role and 3) the feelings that doing their job elicits (valence). The third

subtheme, *Dealing with Professional Identity Tension on a Personal Level,* refers to the identity work they perform when they experience events or stressors inconsistent with their values or their expectations of the role to stabilise their professional identity.

Superordinate theme 1: Purposeful Professional Self	
Subordinate theme	**Key concepts and issues**
1.1 Shared ideology of occupation	1.1 (a) Role and function
	1.1 (b) An analyst by any other name…
	1.1 (c) Values guiding professional conduct: Integrity, Objectivity
1.2 Multi-faceted professional self-concept	1.2 (a) Pride in unique blend of skills and knowledge: Thinking skills, communication skills, same fundamental skills in a new context
	1.2 (b) Personal attributes and attitudes: Growth mindset with willingness and ability to adapt and learn; Tenacity, perseverance and patience
	1.2 (c) Valence: positive feelings, negative feelings
1.3: Using professional identity tensions to grow	1.3 (a) Impression management to counter negative perception of the security function
	1.3 (b) Job crafting and innovation

Figure 19: Superordinate theme 1: Purposeful professional self

Subordinate theme 1.1: Shared Ideology of occupation

In this study, occupation ideology refers to the meaning that the participants give to their work—that set of beliefs on how and why they do their jobs. As an emerging profession, security risk intelligence analysis does not have a generally accepted job description, job titles and set qualification and experience requirements. Therefore, the research needed to focus on what they perceive their role and function to be, their current job titles, what they would prefer it to be, and whether there are any codes of conduct or personal values that serve as a compass for their professional behaviour.

Subordinate theme 1.1(a): Role and function as SRIA in the Private Sector

All the participants exhibited a service-oriented attitude towards their work. They understand their main role and function is to provide a support service to their organisations or clients to enable them to protect assets and people by providing *expert advice on threats and risk*:

> My job is to contribute to my organisation understanding threats, identifying the bad guys and maybe trying to figure out a strategy on how to at least try to prevent them from harming us… (V35)
>
> Protecting the company's assets – that's the most critical part. Not only that, because you're not only looking to defend assets, but also its employees. I would say we are protecting everything: the company's assets, its employees and the clients. (E67)
>
> I see myself as a supporting function in making this organization more secure. And with that, I'm in the front line with regard to the domain that I have been entrusted with. I mean, we are corporate services. We are already in the machinery room of the company. (D74)
>
> There's always a crisis… there's always an incident…This is not a job you do, and then maintain the status quo for the rest of your life. It is always fluid. You're usually in the front line if something comes up. You have those antennas, and they sense first, and then you carry them in the organization. And then that keeps the organization busy for a while. (D72)
>
> When people ask me what I do, I start with "I do research and analysis" because that's what I do: "in-depth research analysis on security related topics with a focus on anything that involves crime impacting the company". It's really where our bread and butter is, criminal impact on the company and that's what it is… research analysis on that… (A34)
>
> Security isn't the bread and butter of most organizations, and with that comes a lack of awareness and a lack of understanding and sometimes naiveté. And I see my role and responsibility as providing to the organization an understanding of the changing and evolving nature of threats and what could cause them harm so that they are able to update their network defences or their security posture so that their stay current with what is out there. (J3) The purpose is for the organisation to understand its operating environment better, to contextualise the space around the society it serves and to give an indication of evolving issues that might not be to the organisation's benefit". (J88, J95)
>
> My mission is really switched almost to sort of a counterintelligence posture. My primary goal is to keep my network safe and use expanded tools I've learned by studying analysis and intelligence analysis to do this. (B18)

Two of the ten participants' role and function only relate to security-related matters (Dave and Emma), while the other eight participants also provide decision-making support to a broader range of clients in the organisation, or as is the case with Celia and Lynn, who work for think tanks that provide risk advice to external clients.

Those participants who have expanded their function beyond the security department share a philosophy that they play a supporting role for the larger organisation in making better decisions by providing them with relevant information on issues that might impact their operations. This second function, *to provide support to decision-makers throughout the organisation*, or external clients, to make better decisions, is either already the function or desired function of the majority of the participants. Celia, who has more than 30 years of experience in the intelligence industry, commented that:

> Well, I would hope that what we do is help businesses make better, more informed decisions. And then if those decisions are more informed, then the expectation is that they will be better decisions… The cynical part of me thinks that what we provide is cover for people's decisions so that they can check the box and say, "Jip, we at least spent time thinking and we consulted with experts. So if the decision goes bad, it's not because we didn't do it the right way. (C18)

Tina, who manages an analysis unit in the security department, stated that her ideal is that her unit provides the type of analytical support service to other functional departments:

> I want our unit to become the basis of informed decision-making throughout the organisation. That's what I think we as a profession stand for… certainly, that's what I try to endeavour towards and everything whenever I'm conducting my work. (T22)

> My ideology would be that we enable and facilitate better decision-making. I would have said perfect decision making, but… (laughs) So my drive is towards actionable intelligence. So that's the ideal outcome. It's not necessarily that what the information that I'm giving or what I'm recommending should be taken, but as long as the information that I've gathered has a "So what?" and the "So what?" leads to something that… it has a ripple effect in terms of action that's taken. So it can never be an end on its own. But it has to enable something to happen within the business itself. So it must be actionable. (T24)

Andy sums his role to provide risk intelligence to different divisions in his company up as:

> My goal is to try and influence our corporate security decision-makers and decision-makers within the business—whether that's commercial or research and development or manufacturing or even our non-security supply chain folks trying to bring them some of that risk intelligence to incorporate into their broader risk picture. (A8, A69)

Kate explains that when she provides geo-strategic advice on whether her company should enter a new market, she thinks as her job being:

> … to help the company understand what's going on in the world and how it could affect them. We want to do the strategic analysis because that's a lot more value to the business, particularly as you can bring up issues or opportunities or happenings early on and give the business time to plan and adapt. (K2).

Vic expanded his support role to his employer's broader risk environment when he did a geospatial analysis project to assist the distribution department in understanding product saturation in the country better. At another time, he conducted marketing research and due diligence of companies and persons for the department responsible for international relations, stating he is:

> … able to offer advice and analyses that contribute to decision making in relation to business decisions that involve in some way reducing or dealing with a potential risk situation to business. (V2, V33)

In addition to these operational level broader assistance to the other departments in the organisation, the participants' value on a strategic level is also evident. Ben is often used in his organisation when strategic planning is done to share the risk and threat scenarios. His ability to do red-teaming is well-regarded in his organisation:

> One of the roles that I played successfully inside my organization is reminding my colleagues that, you know, the adversary gets a vote. They just assume that nothing will change and nothing will go wrong and that they have all the information. And I then do this thing where I tell them, "I don't want to disappoint you, but that's not going to happen the way you figure. These are all the things that could derail that… (B36). I get invited to many meetings that have nothing to do with my particular responsibility because people want to hear the red team perspective from me on what they forgot. (B37)

Subordinate theme 1.1(b): An analyst by any other name…

While all the participants have more or less the same role and function within their organisations, none have the same job title, possibly mainly due to differences in organisational responsibilities, human resources practices or organisational culture. Only Andy's title is a *security risk intelligence analyst*, while four others have variations of "intelligence analyst" in their title:

- Kate is a senior risk intelligence analyst

- Josh is a senior intelligence analyst
- Ben is an information security intelligence analyst and
- Vic is a senior intelligence officer.

The other job titles are information and analysis centre manager (Tina), crime analyst (Emma), consultant (Celia), researcher (Lynne) and the least alike is senior lead security expert (Dave).

The majority of the participants feel that job titles are irrelevant. Dave, who has worked for his organisation for the last 20 years, might have had the most telling reply about the insignificance of job titles for him:

> So, in my career, I've been called a security coordinator… I've been called a security engineer… I've been called a security expert, a senior security expert, a principal security expert, a lead business expert. And now I'm a senior lead security expert… I mean, these titles…they don't mean anything to me. I couldn't care less about the current title I have. Do I care what type of title you have? No! I know what you're technically capable of. I know your capabilities, and more importantly, I know you as a person. So I couldn't care less about the current title you have. (D13)

In a similar vein, Andy is quite vocal about his experience with job titles and ranks and how he would instead focus on the content of his work:

> I don't care about the rank or the name - I care about the actual work that I do. It's about the work, not about my job title or some ego. I think that was the identity thing you're talking about: is it really about the position title, or is it about the actual work I'm doing, and I think people get that mixed up in things. They think they could still do the work with a better job title, and it's not the same. (A90)

Only two participants (Vic and Josh) regard their job titles to be important, mainly because they perceive their current roles to be different from purely an analysis function and the status it might give them in their organisation. It seems as though their organisations are still quite bureaucratic, where being a manager or having "senior" in front of one's job title is necessary to get recognition or be considered expert enough to be afforded attention. They prefer being called *senior intelligence advisor*, mainly to gain access to other business units in their organisations as they are engaged in relationship management in their quest to extend their service outside the security department.

It is telling that participants from South Africa and Germany were not keen to use "intelligence" in their preferred job titles, unlike those from the US, UK and Canada. Tina states that intelligence has a negative connotation in her country, while Dave feels that one should move away from using intelligence:

> So I think we need to move a little bit away from this myth about the word intelligence. It's easily being misused and it's often also misused to increase one's importance… I don't like to be called an intelligence officer because that only raises questions… I am not sure whether this is so important to call it intelligence outside the classical police and military environment. (D13, 89)

For those participants like Kate, who is steering her function away from a narrow security role to provide decision-support to all business units in her beverage company, it is similarly essential to speak to a broader possible client base by removing "security" from their job titles by focusing on operational or general risks to the organisation:

> My job title is senior risk intelligence analyst. It's interesting that you ask about being a security risk analyst because we are really working on as we develop the program is not having security part of our titles and not having security part of our… It is that we think of security as one small piece of what we do. (K2)

Subordinate theme 1.1(c): Values guiding professional conduct

Integrity

Half of the participants were vocal about the values or codes of conduct that guide them in executing their roles as security risk intelligence analysts in the private sector. The first value is integrity. Ben, the cyber threat intelligence analyst, feels that organisations entrust him with sensitive and confidential information and that trust needs to be earned by living out the values of integrity and honesty. He is especially annoyed about how cyber domain vendors or some of his counterparts, often without any experience in the intelligence field, would be drawn into the "fake James Bond" culture:

> Some of my colleagues get a little drawn into, you know, kind of the fake James Bond. They won't share information, and they're exaggerating a little. They're leaving stuff out so that they can look mysterious – it's annoying! (B57)

This focus on *truthfulness* and *trustworthiness* echoes in Emma's words that "Integrity should be priority…*integrity and honesty*" (E67) and in Dave's sentiments that "you need

to have *trust* with those with whom you work. You need to be able to have healthy conflict. You need to take over responsibility and accountability. (D83). Kate is vocal when she stated that being a security risk intelligence analyst is like adhering to an *honour system* as there are no rules that bind an analyst to work in a certain manner. For her, this honour system is also part of not having an agenda when conducting analysis or making recommendations to the organisation:

> It's a bit of an honour system to work as a risk intelligence analyst. We have an assumption that you have that curiosity and those questions and the critical thinking and analysis skills and will then want to apply those in a professional manner, right? Like there's no certification, there's no required experience or qualification. (K53)

Objectivity

Celia strengthened the importance that the participants assign to objectivity as a way to conduct their work by stating that it's essential for her to be apolitical, non-ideological and the *voice of reason* when she conducts her work. She aligns herself with the philosophy and values of Stoicism:

> I really admire stoicism as a philosophy - the Stoics. I like to think that my value system is kind of carved into that template… what I get out of it that applies to risk analysis… is that Stoics try to keep everything in perspective, everything in its proper proportion. I try to be the voice of reason - I'm trying to be calm and the voice of reason… I very much strive to be not ideological. Which is another way of controlling, say, in a more meaningful kind of control of your biases. (C25)

The need for *objectivity* is strengthened by Celia, who uses the example of a Pulitzer prize-winning journalist to contrast how SRIA would conduct their work by stating that analysts do not have or should not have a vested interest in a product and therefore does not need to highlight specific areas to drive a particular agenda.

> When they decide on a story, the Pulitzer Prize journalist gets really invested in that story and pursues it. You know they're often discovered, some of them, to have exaggerated the story. Or got a little light on the details, right? And I believe ideally we do not do that. If there is no story, there is no story there. We're not invested in it. We really don't care. We'll move on to the next story. (C21, C22)

Kate and Andy reinforced the notion that the analyst's value of objectivity should become the hallmark of their conduct in the workplace:

> …the nice thing about being the intelligence analyst is you can be the one that brings information relevant to everyone but doesn't have an agenda. (K18)

> The analyst is supposed to remove the bias, look at the facts, and then make an analytical judgment based on the facts. If we could learn anything from our roles, if we could promote anything about the position, it's about candid, unbiased analysis, and that's what leaders want. I mean, nobody, leaders, don't want things sugar-coated; they don't want things derived from an agenda. (A96)

Subordinate theme 1.2: Multi-faceted professional self-concept

After establishing what the participants view to be their role and function, how their organisations and themselves name their function and what they perceive to be the profession's values, the analysis moved to determine how they perceive themselves, on a personal level professional role. This subtheme identified the tenets of individual professional identity, which is influenced by 1) their *skills and knowledge* they apply when executing their roles, 2) their personal *attributes* and *attitudes* that they perceive to play a role in their professional experience, and 3) how they feel (positive and negative valence) when they execute their professional role. As could be seen from the demographic analysis, the participants have a wide range of different life and professional journeys (combining a total of 209 years of work experience of which 82% or 171 years are in the intelligence or security risk environment), which resulted in a rich and multi-levelled analysis.

Subordinate theme 1.2(a): Pride in a unique blend of skills and knowledge

The participants were vocal about what they perceive as their unique sets of skills and knowledge that enable them to perform their work effectively. These skills and knowledge can be broadly grouped in 1) thinking skills, 2) communicating skills, and 3) the cluster of contextual understanding skills that enable them to excel in the private sector workplace.

Thinking skills

The participants first take pride in their thinking skills and use this intellectual ability to earn a living. Celia articulated it well by saying:

> I think of myself as a professional thinker. That's really what I am. But what does that mean? I'm a professional critical thinker. So that means I can evaluate information for its value better than other people… I'm more aware of my biases than other people, and I can correct them better… to me, a real intelligence professional is aware of his or her biases and other people's and has developed heuristic thinking methods that allow them to get closer to the essential facts of the matter. Better than other thinkers... (C10,16)

Similarly, Ben realised that the value he brings to his organisation is "to think clearly. And "I was succeeding in the sense that my analytic skill was in high demand across the organization." (B46,47). Other participants have also stressed the ability to think critically. Kate thinks asking questions and challenging assumptions is the essence of their roles:

> Analysts… we're critical thinkers… being the ones who ask questions, challenge assumptions and bring together the information that I think that's vital for society. (K18) We are the people who ask questions without an agenda. (K24) …my space is asking questions, trying my best to figure this out, hold this puzzle together… (K33)

Other participants mentioned their *ability to think at different levels of analysis* by applying their strategic, operational, and tactical thinking levels to understand a problem and provide effective recommendations. Emma and Ben illustrated this when they said:

> I come from a diverse background and experience. If you take all of it into account, being operational, tactical and strategic - you put those three into one – so it brings a lot to the table in terms of how I look at things in my current space. (E13)

> And I can, because I have a lot of business experience, bridge the gap between my technical security issues and how that relates to financial and business risk issues. And I'm good at switching between a high-level strategic view and an operational view… how those sort of the larger ones might actually impact things at the university. (B24)

Tina uses the puzzle metaphor to explain the thinking skills necessary to execute her task by saying:

> …it's exciting to be looking at an issue… to get to the bottom…. to get to the "so what?" to put pieces together ... to view it as a puzzle and say you'd like to resolve it and give a full picture. (T12)

A related thinking skill is to *discern macro-level patterns or events* that may be of importance and *sensibly ascribe meaning* to them in a certain context. Celia feels that this is her unique contribution:

> My comparative advantage…and what I'm good at is noticing weak signals from multiple sources and figuring out what possible emergence they can contribute to. (C10) and "I have a sense which I think is important… of macro trends in the world. Not just the micro particulars of a given situation. (C16)

Dave also feels that this *sensing or identification skill* is essential to his work by stating, "you have those antennas, and they sense first, and then you carry it in the organization". On a more operational level, Andy used the metaphor of "needles in a haystack" when he described his experience of looking for specific pieces of intelligence when he was in the military and now still uses the same skills in the private sector by saying:

> The best way to explain it essentially is the proverbial needle in a haystack. So in the military, you have to find that needle faster; that's the key. So I think in the private sector, we don't have to find that needle as fast, but I still do that because of my military experience. And the needle is essentially the "So what?" like you're thinking, "why is it significant?" It comes down to that; you go in the haystack and get it. I mean… find that needle, understand what it means to get it to where it needs it to go. That's what it's all about. I feel like I have an advantage because I understand it's really about focusing, identifying, understanding what's important, why it's important and get it out to whoever needs it. (A59-61)

Communication skills

The *ability to communicate well* seems even more critical in a work context where one's stakeholders do not necessarily understand your role and what you bring to the table. Vic stated that he could communicate better than most other people in his environment when he said:

> I also bring the ability to communicate in a clear manner that's understood by a non-security risk professional. I found that that's a unique skill that often security types or people who do analysis cannot communicate relevantly to the business, right? (V31)

Vic explains how his ability to communicate well also assisted him in information gathering by "talking to people, attending meetings, walking around and trying to

identify threats in the environment" (V4) and "discuss the issue or I might say "hey, do you know anything about this or about that?" (V6) and "I like the social element, and I like the liaison." (V50). Kate's skill to write and communicate well has been highlighted as essential skills for any intelligence analyst (K54). Josh sees his ability to use language as tradecraft to influence decision-making in his company:

> You already know the discipline of threat… you have the language. It's like you can do what you want with language. If something needs to sound more serious than it is, it can, without being dishonest, if the desired outcome is a change of behaviour from senior leadership and if that means you have used a certain type of language, and then you use that type of language without being dishonest. Well, actually, the power of intelligence is to influence decision making. And it's not being dishonest. If you have what type of decision will bring about a reduction of risk to the organization, and how can I help facilitate that? So, I don't see that as being dishonest. I see it as an extension of tradecraft. Like in the same way, if we were in other sectors, we would see tradecraft is what we do. What about when we go into the private sector? What is intelligence tradecraft about? It's probably these types of things. (J47,48)

Same fundamental skills… in a new context

From the above, the analysis revealed that the participants are critically aware of their work context and employ various skills and knowledge to ensure relevancy and legitimacy in the private sector context. Andy, Tina and Josh were specific about the application of their *intelligence analysis skills* and their understanding of threats in the new private sector context:

> I think what I've learned is this position is less about being a security analyst; it's more about being a research and analysis professional. You can take your research and analysis skills set and apply it to pharma. (A13)

> So it's really about focusing, identifying, understanding what's important, why it's important and get it out to whoever needs it. So basically, you're taking the fundamentals and overlay them on a new data set, instead of counter-terrorism, its pharmaceuticals or whatever. It's the same fundamentals that you overlay onto new types of missions. (A65)

> What we do is actually more of a transdisciplinary skillset than an actual discipline. Because we would be able to do whatever we do, we can do it in whatever field. (J98)

> I think what we bring to the table is an understanding of the adversary mindset… whether it is a nation-state or a particular group or an

> actor…about what actions they want to do and how they would be able to do that. (J40)

The participants highlighted how they have to *understand the business of the organisation*, its operational risk, the stakeholders, its supply chain and internal politics to provide a relevant risk intelligence service. They had to relook their approach and learn new or apply existing skills and knowledge to do their jobs effectively. Kate stated that she had to *research and analyse* her employer to be able to identify what intelligence needs they might have so that she can provide that service to them:

> I changed the way I think about my work. Instead of being a good intelligence analyst, I changed my focus, and I tried to really take the skills and apply them to the work… which is why I think I could really understand quickly that I needed to know how my company works to do my job. (K45)

Good communication skills align with one's ability to manage relationships with stakeholders in the company. For Kate, an essential component of communication skills can identify one's stakeholders "to know whom to talk to within the company, even who in the company will be the end-user of your work or your product" (K8). She sees her skill to "help people understand what they don't even know they want" (K28) as one of her strengths when she communicates her vision to extend her risk intelligence service to the broader organisation:

> Our job is to tell our customers what they want, that they don't know they want. And I am perfectly comfortable going out there and knowing that I have to convince someone that what I am giving them is what they want, not necessarily what they asked for. Or give them something they've never even heard of. To me, it's fun. (K20)

Vic summarises SRIA skills and knowledge as the ability to identify threats, relate them to the business interests and communicating the risks to enable decision-making:

> I guess my speciality would really be identifying and linking issues that are not obvious and being able to go in-depth and really understand how a business works and how the external environment can affect some internal business operation inside… and communicate it in a clear manner. (V31)

Subordinate theme 1.2(b): Personal attributes and attitudes

The participants shared certain personal attributes and attitudes relating to their professional role that they perceive to be essential in their lived experience. The participants exhibited different personalities but related some attributes to have moulded who they are as SRIA in the private sector.

Growth mind-set

The most common attribute shared among the participants is that of a growth mindset with a willingness and ability to adapt and learn. It most probably relates to their quest for intellectually challenging situations and roles to apply their thinking skills and learn new things. Dave, Tina and Kate illustrated how they enjoy working in an environment that changes all the time:

> When I come to the office, it will always be interesting. I have not had a single boring day in those 20 years of service, not a single one. (D34)

> There's always something… It never gets boring…There is always a crisis… there's always an incident, there's always an item that is new, and you're constantly learning. This is not a job that you do and then maintain the status quo for the rest of your life. It is always fluid. You're usually in the front line if something comes up. (D72)

> So no two days are the same, no two hours are the same. So that's what keeps me going. (T30)

> It's a continually evolving process. The business evolves, the business makes changes. We have to be able to learn and evolve with it. (K14)

Similarly, Lynn liked constant change stating that "I have a very low boredom threshold. I mean, I don't see what's the sense of doing the same thing over and over for years." (L32). Vic concurred with the issue of boredom by stating that he needs variety and intellectually challenging work "if the job is narrow and it's the same and repetitive, I get bored, and I want more variety and personal fulfilment." (V57) "In my previous role, I did the same job for about six years… and I got bored of the subject matter that I was analysing and at the time, I didn't have enough self-patience." (V22) Emma was the only participant who felt that her current role did not provide sufficient growth opportunity and indicated that she wants to do a different kind of job:

> I want to branch out from what I'm currently doing. I've done analysis for over 15 years now. Now I want to go into something new to do with investigations. (E2)

This attribute to *adapt to continuous change* is closely related to the *willingness to learn, improve continuously and expose themselves to other opinions*. This attribute was a common thread among the participants. The word "learn" has been found 37 times in eight interviews, with Vic using it the most (15 times), Andy (6), Ben (5), Celia (3), Kate (3), Josh (2), Emma (2) and Dave (1). Vic's growth mindset is evident throughout his interview. He mentions his eagerness to learn what intelligence analysis is as the main reason he decided on this career path.

> What drove me is the mystique and the mystery of it. And it sounded interesting and difficult… So what drove me is why I want to learn about it. I wanted to find out about it, and I wanted to see how it's done; I wanted to see who does it and how to do it. (V142)

Andy and Emma's ability to learn and adapt was evident when they learned how to support the business areas with their risk intelligence analysis.

> Where the support infrastructure allows, you can really learn a lot about a topic, you can really dive into it and I kind of like that ability to know more about the topic than just make a decision on… I like to know more. I like to dive into it and get a better understanding, even for my own benefit. You know, I got to see interesting stuff; I just want to learn more about it. (A72)

> I have tried to learn a lot of other things in the process. Instead of operating from a laptop… of what you see in a formal report, I'd rather go there physically and check what is happening. So that added more value to what I'm doing. It is something that is very special. (E15,16)

Tenacity, perseverance and patience

A second shared attribute is that of tenacity, perseverance, and patience required to do one's job as a security risk intelligence analyst. Andy stated that "…it's really hard work we're doing. And it's hard trying to stay on top of things if you can persevere through the end result whether that's a good case you resolved, or you've influenced a business decision." (A40). He found the task of staying abreast of developments across many intelligence priorities intellectually challenging but fulfilling when he used that knowledge to achieve impact. Tina concurred that one would need hard work and

perseverance to execute this role (T38). Lynn echoed this when she stated that one needs "lots of patience" to do this job (L24) and that her task to develop a database of piracy events from multiple primary and secondary sources to then only start the analysis and writing process is "extremely time-consuming" (L26). She shared her frustration at researchers who do not need to do this grunt work or stakeholders and clients who do not have an inkling of how long the process takes to understand a problem and then look at how it can be presented to make actionable recommendations. She eloquently explained it as "I think analysts and the people they work for, need to know this is not fast food, this is slow-cooked…" (L44)

Andy, who was very vocal in his perception that his role is a supporter of decision-making, reflected that *humbleness* is an important attribute for him. He discussed how he realised that being an intelligence analyst, both in the military and the private sector, is like being a "worker bee". "I've always been a worker bee. I'd rather do this work… I guess it's more about the work than the position." (A86, 87). Further to this metaphor, he feels it is necessary to be humble "I think if you're humble enough to understand that even though you've done a bulk of the work that the lead investigator may be briefing it, and you know, getting a lot of good feedback, you have to find satisfaction in that…" and "I think if you can be humble enough, it can be very satisfying". (A38-40)

Subordinate theme 1.2(c): Valence

Positive feelings

Positive and negative emotions play an important role in creating and maintaining a professional identity. In this study, the narratives of positive feelings far outweighed those that reflected negative feelings. The majority of the positive feelings related to pride in their intellectual abilities and their feelings of fulfilment and job satisfaction. It stands to reason that as the participants' main skill relate to their perceived ability to provide professional thinking skills, it is also this cerebral ability that elicits feelings of pride, which might be interpreted as arrogance if it were not applied to a "greater good" and not for personal gratification and benefit. Celia stated, "It feels good to think of myself as a good thinker" (C31), while Josh was a bit more modest when he said that he

> "… felt privileged to be able to try and understand quite intellectual topics like geopolitics and political tensions and the strategy and these types of things. I do enjoy it…to talk about what's happening and try and make sense of it. That feels good". (J36), and "I like the variety of work. I like the subject matter… the intellectual aspect of it." (J62)

Vic likes the freedom that his organisation gives him to do his job without restrictions.

> I like the freedom of identifying and researching. I like not having restrictions on a specific theme or specific area… I like the ability also to talk to different people on different subjects, different current events. I like the variety of the work. (V46)

He then pushed the envelope when he stated his preference for working with complex issues rather than "petty, straightforward issues that can be handled by someone junior… I prefer to deal with something a bit more complex that's maybe multidimensional and worthwhile and something maybe that even engages multiple stakeholders." (V79)

Some participants derived pleasure from having access to sensitive information or to have intimate knowledge about threats and risks that are people rarely would have access to (or interest in). Andy likes the idea that he knows what is going on, regardless of whether he is a decision-maker or a worker bee, "you always have your finger on the pulse of what's going on. And you're always in the know…" (A67) Dave exhibited the same emotions of exclusivity when he stated that he likes finding something that no-one else has found before:

> Well, the motivation is that you always have a little flashlight and a dark room where you try to light up that room, *and you always find some dark corners that nobody has found before*. It is so interesting ... (D42)

These feelings of accomplishment may come over as elitist, even arrogant. However, the participants' knowledge and thinking ability are valued and respected by their colleagues and stakeholders. Kate said that she "feels respected and that people see my value" (K51). Lynn says that she gets recognition and that her work has been published on BBC, Forbes and the Economist (L38), while Josh said that his opinion is often requested "as you're the subject matter expert." (J77)

Participants expressed feelings of job satisfaction, stating that their work is meaningful, not only to them personally but also to their organisations. Kate and Emma had fun and was grateful to contribute to something worthwhile. “I enjoy doing this… I have a lot of fun… I get to do my best in what I'm doing… “(K33) and “It gives me pleasure to know that at least I can contribute towards protecting the bank’s assets, its employees and our clients. (E11) Ben’s happiness with his role as a security risk intelligence analyst was especially powerful when he stated

> Oh, It's just the most creative and engaging, challenging, fun work I've ever done. I personally feel I'm able to sort of use all of my gifts. You know, I get to do a little of everything, and I love it. (B39) I think that real satisfaction in your work… just raises the tone of your life, and it allows you more resources to be kind to your family and the people around you. (B44)

Negative feelings

Overall, the participants did not exhibit negative feelings about their profession or role as SRIA in the private sector. Negative valence was evident in only two aspects, namely, where participants had negative feelings towards their perceived image of working for a security department in the private sector. Secondly, the organisational culture could not effectively deal with gender and race issues.

Not all participants who work in security management departments had the same negative experience that individuals like Vic had as the organisational culture, and even personal aspects such as emotional intelligence might differ. The essence of the negative feelings centred on perception inside and outside the organisation that being part of the security department is of lesser importance or value to the organisation. Vic illustrated this perception explaining his culture shock when he came from an environment where intelligence was the core business into a function that was situated in a support department:

> In the military or in the defence where I came from, security is really seen as a dirty area…Where you know, those who didn't make it or didn't have education would go there. All those security people are sort of the low level… sort of the uneducated, inexperienced, stupid sort of unprofessional security guard. So I came into this job with a very negative

> view of security and the people who were just out to get you for no good reason, not to help you or to facilitate you. (V87,88)

Some female participants found their workplaces dominated by former law enforcement and military males, who imprint their preconceived ideas about intelligence analysis into the private sector and their outdated racist and sexist mental models. Emma shared how the security department in her workplace is dominated by former police types who could not understand her role and where she had to teach them how to write reports on incidents to build a database. She also mentioned that she finds many challenges as a black female where her initiatives are stone-walled by her male, white colleagues. Celia shared how her professional identity has been impeded by the mental models of those in the intelligence community who expected her, as a Latino woman, to be a South or Central American expert while she wanted to work on China. Also, the way she looked did not match their idea of a professional, and she thinks that affected her professional trajectory:

> So the man in the crisp suit and the crisp tie - that's an expert. The woman in a dress and wearing jewellery does not look like an expert. So there's that issue, right. And so I felt that my contribution was undervalued… (C43) I mean, someone has to say that being a woman can lead to earning many problems for you... (C50)

Subordinate theme 1.3: Using professional identity tensions to grow

Most of the participants' professional identity was challenged in various ways, but they acted with self-awareness and reflected on their circumstances and their professional ideals, and where necessary, actively performed identity work. Those who moved from the intelligence community to the private sector experienced a massive culture shock, which required intensive professional sensemaking and recalibration. They were confronted by a perceived lack of legitimacy, as they now had to justify their roles, while it was never necessary for their previous roles. Also, very few of the stakeholders understood their function and the value they bring to the organisation.

This prompted them to reinvent themselves and use their skills and knowledge in their new context to attain legitimacy in the organisation. Both Dave and Andy had no issue professionally because they are situated in a support structure. As seen before, Andy

saw himself as a "worker bee" that knows everything that is going on, and that is sufficient validation and work satisfaction for him. Likewise, when asked whether he minds being in a support role, Dave saw himself as playing a leading role in the support department of his organisation, and that is sufficient validation for him:

> I see myself as a supporting function in making this organization more secure. And with that, I'm in the front line with regard to the domain that I have been entrusted with. I mean, we are corporate services. We are already in the machinery room of the bank. (D74)

Subordinate theme 1.3(a): Impression management to counter negative perceptions of the security function

The most explicit professional identity crisis was shared by Vic, whose professional identity is closely linked to how other people perceive him and how he feels when he works. He explained he moved to the private sector for a higher salary and senior analyst position. His main professional identity challenge in the private sector occurred when he had to deal with his own and others' negative perception of people working in the security department as a subdivision of the overall support services:

> I started to think that this is maybe not a career or a respectable career …it's a highly peripheral central support service …you're not core business. You're perhaps sometimes not even enabling core business… yes, you're keeping people safe and everything… (V87). I'm not proud to say I work in the corporate services department. Through most of my career, that's the paperclips and paper and toilet cleaners right? No really! So I actually am very conscious of that and focus more on the actual work area. (V110)

He used a dual approach to manage the tension he experienced: firstly, he disassociated himself from those in the security department that was known to "aim to get you on a security violation" (V88) by making sure that he is never seen in their company:

> I just didn't want to be seen hanging out with them and be buddy-buddy, at the coffee stand, at the cafeteria - I didn't want to be seen hanging out with them, so I would only transact with the No-Sayers as required. (V40)

He even went as far as redesigning his email signature by "removing corporate security service depending on the audience of my email." (V110). In his interaction with people from outside the security department, he deliberately portrayed himself as different from his security colleagues:

> So I branded myself internally as not that guy. So I don't … none of the advice I provide is framed in a way that would restrict someone from doing something. I've also physically distanced myself from people, other security professionals in the bank who are the No-Sayers and No-Doers. (V38)

These identity protection strategies is typical to control others' opinion of oneself for a personal purpose. In Vic's case, he both disassociated himself from a certain group of people and employed impression management to be accepted professionally and to ensure that professional interaction with those he perceived important for his professional well-being goes smoothly.

Subordinate theme 1.3(b): Job crafting and innovation

Emma became operationally involved with the investigators to understand their context and make recommendations that are valued and executable. Andy explained how he used to have ten analysts working for him in the military, and suddenly, he has none and had to change his expectations and adapted to the organisation's pace and context:

> I think the challenge was reinventing yourself on how you execute your work. I really had to reinvent how I work … understanding they're (consultants) not going to get me intel - finished like my analysts would do in the Military. That really was the big challenge. (A92, 93)

The participants faced their professional identity tensions with creativity and crafted a new role that stretched beyond the job description for which they were appointed. Emma and Lynn developed new databases, while Kate, Tina and Vic immersed themselves in understanding the business better to extend their intelligence service to a wider audience in the company. Initially, Ben was frustrated when he was being pulled into side projects that had nothing to do with his role, like "ghostwriting his boss's presentations". He wanted to spend his time and energy on new threat analysis but never had the time to get to it due to his other, unrelated responsibilities. He did some introspection and

> … realised that I was succeeding in the sense that my analytic skill was in high demand across the organization. But I had narrowly defined the value that I brought to this particular arena. So I was unhappy for a while because I wanted to perfect something instead of maybe being more generous - you know, use skills that the organization had afforded me more broadly than in a less narrow way. The challenge for me has been

> to realize that my value to the organisation is my value to think clearly. (B46-48)

Vic also managed the professional identity crisis by looking at ways to rise above the perception of his work context. He creatively extended his client-base and deliverables by deliberately seeking opportunities to give him exposure to other parts of the organisation, leading the organisation's international liaison in security risk and intelligence matters and offered to work on large projects with colleagues who are certified security professionals. His manager supported these activities, which served as validation for him. It can be surmised that Vic focused now more on the value he can bring to the whole organisation than where his structure is in the organigram.

As can be seen from the above analysis, each participant had a unique professional journey and life experience that influenced his/her security risk intelligence analyst identities. Their job titles might be different, but they share the same ideology of their profession in terms of their role and function and what values guide them in executing their tasks. The multi-dimensionality of their professional self-concept was highlighted by their unique analytical, thinking and communication skills.

Overall, they ascribed their perceived professional success to a growth mindset that values change and learning and being in a role that fosters change and provides plenty of opportunities to learn. The participants overwhelmingly portrayed positive feelings of pride, fulfilment and job satisfaction and dealt with professional identity tensions in creative ways that enhanced their role and impact on the organisation.

5.5.2 Superordinate theme 2: Connectedness to others in a professional context

One of the core dimensions of professional identity is the enacting of belongingness or connectedness to people who have the same professional function as you do, with a sequential “otherness” to people who have a different vocation (see Figure 20). The analysis of the interviews revealed two subthemes. Firstly, the participants strongly identify with others who perform similar functions in the private sector, but more in a network context rather than in the context of traditional professional bodies. Secondly,

their interaction with others in the work context is complicated by a continuous explanation of their role to gain legitimacy and acceptance.

This could be ascribed to stakeholders' unfamiliarity with the emerging profession, which, in turn, led the participants to craft and enrich their jobs to achieve the opportunities in the workplace. Consequently, the participants adapted and strengthened their professional identity to become and remain relevant in the work context.

Superordinate theme 2: Connectedness to others in a professional context	
Subordinate theme	**Key concepts and issues**
2.1 A network rather than an association	Functional networking No need for professional organisations Social media
2.2 "Prove that you are a business enabler."	Lack of knowledge about function leads to misunderstanding Educating stakeholders Building nurturing relationships

Figure 20: Superordinate theme 2: Connectedness to others in a proefssisonal context

Subordinate theme 2.1: A network rather than an association

It is relatively easy to have a sense of belonging and connectedness in established professions such as accounting, health and legal professions where there are role models and standards of behaviour or professional organisations that embody legitimacy. However, in an emerging profession such as security risk intelligence analysis, there are no prototypes or standards, and the participants of this study are testimony of learning while they are doing. There are also limited opportunities for SRIA to embed the social aspect of their identity as there is at this stage, only one professional organisation that addresses the needs of risk intelligence analysts in the private sector *per se*, namely the Association of International Risk Intelligence Professionals (AIRIP), which draws most of its membership from the US and Canada.

Half of the participants are the only analysts in their organisation, while the other half works in teams of analysts. All of them, except Emma, who works as the only analyst in a commercial bank in South Africa, has contact with counterparts outside of their organisations, mostly only on a professional and not social level. This networking and liaison with analysts in other organisations serve as a valuable reinforcer of professional identity and exchange of ideas. The participants explained how insular it could become when you do not deliberately network with analysts outside your organisation and feel more job satisfaction if your counterparts value your opinion or analytical products. As they all value their ability to think critically about the issues they analyse, work-related networking serves mainly as a forum to test their insights against those whose critique they value. Vic even went as far as making this liaison with his counterparts in other organisations and other parts of the world the main deliverable of his function.

> I like the social element, and I like the liaison. And in fact, I told my boss… I said as a joke, and I said, "you know if you limit me in my networking ability, or if I'm not part of any working groups, I'm out of here."(V50)

Being a member of a professional organisation is not important to the participants, most probably because they find sufficient networking opportunities while doing their jobs. The four participants who are members of professional organisations find it useful for different reasons. Andy, Kate and Emma network with other risk intelligence analysts to ensure that they know what is happening in the industry and make contacts for possible future employment opportunities. Three other participants (Tina, Josh and Vic), who are not members of professional organisations, feel that networking through these bodies can be beneficial but have not yet made an effort to join or start such a body. Dave is outright dismissive of professional organisations as he "doesn't need to sell myself" (D85). Ben's networking experience in the intelligence field has been positive, but he experienced exactly the opposite in the cyber intelligence field:

> … it's a combination of … anxiety and egotism… everybody wants people to feel a bit of schadenfreude—like, you know, you made a mistake, and I could catch you. It's not constructive at all. And you know it's profoundly unkind, and it sure as hell is not moving the discipline forward at all. I see a lack of kindness and collegiality already bring the whole enterprise into disrepute. (B60)

Connectedness with other intelligence analysts is also strengthened by some participants' membership of online social networks like LinkedIn and Twitter, although the engagement is limited to receiving posts and sometimes offering inputs. Only Celia, who is at the end of her career, engage more robustly on social media, but with a specific mentoring role:

> I get on social networks, particularly LinkedIn and Twitter. They tend to connect with me. I don't tend to connect. I'm at the end of my career. I'm not trying to build anything, but particularly the younger analysts will find me, right? And then start engaging with me and ask me to comment on this or that. And I'm very happy to do that. That's…what I feel like that's my proper role now. You know, generationally, that's what I should be doing. And so I do feel connected with them that way. (C28)

Celia is the only participant involved in other initiatives to strengthen the intelligence field through her leadership role in a mentoring network for women in intelligence and representing intelligence as a discipline at interdisciplinary research institutions.

Subordinate theme 2.2: "Prove that you are a business enabler."

As previously stated, the participants shared a service-oriented ideology of their work. They understood their main role and function to provide a support service to their organisations or clients by protecting assets and people through expert advice on threats and risk. The participants need to connect with stakeholders inside and outside the organisation that will enable them to fulfil this role. Dave succinctly linked his professional identity to his ability to relate to stakeholders in a manner that helps them to do their jobs better:

> So I think the identity would be established if you can prove that what you do is a business enabler, not a business hampering effort… People should realize that what you do actually contributes to their success. (D80)

However, initially, stakeholders do not understand intelligence and what value a SRIA can bring to the organisation. Kate and Josh's frustration with the lack of general knowledge of intelligence and its role in the private sector was evident:

> Society does not have a great understanding of what we are. I mean, if you talk to people, their conception is government intelligence is spies, right? Their reaction is, "that's a thing?" Or they might think it's more like corporate espionage. (K24)

Tina echoed a shared frustration that people see that you are a good report writer, and could therefore push you into a clerical role if you do not explain your role and function outright and with confidence guide their expectations:

> So expectations sometimes are misguided… and what is expected of us as an output actually doesn't talk to who we are and the role we are here to fulfil. So sometimes, we are requested to give clerical support function instead of proper analysis and input towards, as we said, strategic decision making. So that's frustrating. (T48)

Participants only made an effort to explain to people their role when they were stakeholders or potential clients of their professional services. Most participants omitted to identify themselves as SRIA when meeting people socially. They were not ashamed of their profession, but they did not feel it was relevant or necessary to the discussion or thought it might elicit questions about sensitive or confidential issues. Dave joked and said he would tell people he is a well-paid kindergarten teacher, but on a more serious note, he stated that he would tell people that he works in the administrative part of a bank, which sounds "boring enough to steer the conversation away" from him. Emma never told anyone what her work is because she does not think it is safe to do so, while Vic would tell people that he deals with "specialised operational risk". Andy would tell people that he does research and analysis, and that would usually end the conversation because it does not sound interesting to the other party. Both Josh and Ben would say they are cyber threat intelligence analysts because it has become a familiar role in the last few years.

However, when the participants encountered stakeholders in their organisations and related industries, they were very clear about who they are and their role. The participants were eager to share how they educate the stakeholders, with Josh even accepting it as "part of the tradecraft path of enlightening and explaining" (J80). The participants do not have to justify their existence, as their organisations already decided they need the function, did a job analysis and went through the recruitment process. However, the challenge is to ensure that they add value and are seen to be valuable to the organisation by the stakeholders.

Kate has a similar approach where she deliberately went out and learnt as much as possible about the organisation to determine how she can provide better decision-support:

> Well, look, I'm part of a new team, and my job is to support you. My job is to give you the information that helps you make the decisions you want to make. I'm not making any decisions for you; I'm not telling you "No", I'm not telling you "Yes" I'm not telling you "well only if…" I'm just telling you "Here's information to help you make your decision. What information do you want to know?" (K13)

SRIA should also be competent in interpersonal relations within an organisation. As their main business objective is to influence decision-making by providing unbiased decision support, it requires advanced self-awareness and facilitation skills. In terms of self-awareness, the participants shared how they build meaningful relations with stakeholders by being humble and approachable. Dave was self-effacing to get their cooperation or collect information from them:

> I never take myself too seriously. Meaning I would rather surprise somebody…I play a bit stupid at the beginning… the Colombo approach. People are immediately willing to help. But if you come into the room like an elephant, people don't want to help or listen to you. (D97)

Josh reiterated how he approached stakeholders explaining to them the significance of his role and building a trusting relationship with them where he had to prove himself to be credible and trustworthy:

> And just having an understanding of their world that's been key to building those types of relationships, and that's something that the organization didn't necessarily have. (J50) Without credibility, then you know… what you're saying has to be taken seriously, has to have some substance, and has to have some influence. You can be the best intelligence analyst, but maybe like any other job, if you lose credibility for any reason, that diminishes. The approachability, I think that's just a business skill in any organization - you need to have that. If someone doesn't like you, they are not going to listen to what you say. If they do like you, they will fall off a cliff if you say so. (J105)

As with any other profession, the participants faced challenges with interpersonal relations at work. Dave was perhaps the most cogent on how he dealt with obstacles in the workplace pragmatically and professionally:

> My colleagues are not part of my frustrations at all. If you're walking down a certain corridor and it is blocked, you can either continue to run against that wall or find another way. So I'm not dogmatic. You know, I do whatever this organization asked me to do. I'm being paid very well. So why should there be frustration? (D64)

In summary, participants' professional identity is not dependent on the existence or membership of a professional body or socialisation with others in the same profession. Neither do they need the validation of the general public of their professional status or legitimacy. However, they value the occasional functional interaction and liaison with counterparts on a professional level which reinforced their professional identity and sense of belonging. When confronted with ignorance of their role in the organisation and the possible hampering of their function's execution, they deliberately and professionally connect with stakeholders to illustrate their value to the organisation. They are pragmatic in their approach to nurture relationships with stakeholders and willing to adapt their functional scope if the client requires it.

5.5.3 Superordinate Theme 3: Professional Identity Enactment in the Workplace

Professional identities are primarily constructed and maintained in a professional workplace context. It, therefore, stands to reason that the participants' day-to-day lived experience would be impacted by their organisational habitus, specifically the dynamic interaction between them and the organisations for which they work. Three major themes were identified on how their work environment enabled or frustrated their quest for meaningful work (see Figure 21 below). The most common theme was how the embedded organisational culture, or "the way we do things here", influenced how they practice their professional identity daily.

Superordinate theme 3: Professional Identity Enactment in the Workplace	
Subordinate theme	**Key concepts and issues**
3.1 Organisational culture is paramount	3.1 (a) Organisational identity
	3.1 (b) Values and behaviour
	3.1 (c) Leadership
3.2 Organisational structure restraints impact	Matrix model most appropriate, In-sourcing
3.3: Inappropriate HR practices	Recruitment, career pathing

Figure 21: Superordinate theme 3: Professional identity enactment in the workplace

The organisational culture subthemes included the impact of organisational identity, the values and behaviours that enable their professional enactment, and the impact of managers and leaders' actions on their job satisfaction and, ultimately, their professional identity. The second theme dealt with the challenges they faced when confronted with negative perceptions about the security departments' place and role in the organisational structure and the associated power and image implications, limiting the impact they think they have in the organisation. Lastly, the participants shared how damaging inappropriate or ill-advised Human Resources practices can be to enact their professional identity.

Subordinate theme 3.1: Organisational culture is paramount: "This is a great team to be the goalie for"

Organisational culture is a complex combination of values, behavioural norms, artefacts and patterns of behaviour—"who we are as an organisation and the way we do things here". The interviews' analysis identified a few subthemes that can be grouped in the broader organisational culture subordinate theme. These are 1) organisational identity, 2) values and behaviour and 3) leadership.

Subordinate theme 3.1(a): Organisational identity

As seen in Chapter 2 of the thesis, organisational identity is the individual's sense of belonging to the organisation for which he works. The participants exhibited various degrees of association with their organisation, which could reflect what extent they choose, or are able, to enact their professional identity in that organisation. Two of the participants (Dave and Ben) exhibited a very strong association with their employers, which enjoy high public regard for their role, values and impact on society. Dave outrightly stated that his organisational identity is stronger than his professional identity when asked which identity is the strongest. He reasoned that the organisation afforded him opportunities that he would not have had in other organisations, and he, therefore, "totally identify myself with the shop". (D87) As seen earlier, Dave also exhibited the least preference for a job title when he shared the many titles he had for the same job in the last 20 years.

Ben shared his high regard for the organisational values and the impact the research university has where he works as the cyber threat intelligence analyst. He is especially proud to be associated with an organisation that is at the forefront of scientific research, and he feels his job is to protect the network so that the researchers can do great things that matter. His values are embodied in the organisational quest for humanity, and they allow him to contribute to this through his role and make his work meaningful. He even went so far as to say that his work allowed him to be a better person.

> I knew I could make more money elsewhere. But this is a great team to be the goalie for. This organization has given me the latitude to actually help. I'm sure you get involved in organisations where you can make more of a difference than you are allowed to. But this organization will actually let me help… the organization had afforded me the opportunity to use my skills in a more broad way than in a less narrow way. I think that real satisfaction in your work, you know, just raises the tone of your life, and it allows you more resources to be kind to your family and the people around you. (B42-46)

Josh shared that his organisational identity in the private sector is also relatively strong, despite him having more "purpose" when he took abusers, terrorists and drug pushers "off the streets" when he was in law enforcement. He exhibited self-awareness that he might never again feel "really dutiful" or the same job satisfaction in other organisations. But he can associate himself with the values and purpose of his new organisation because it provided him with other professional identity benefits that he did not have in law enforcement.

> I think that in all honesty, there is an element of that (working in law enforcement) that you're not necessarily going to get from other types of organizations, and that's maybe just a reality. Now that I'm in the bank, you know our values… it's about promoting the public good and acting in the interest of the citizens, of financial stability and yes, these things… and that ideology is sufficient for me… it's not the same as what I did before. (Job satisfaction) is different. It evolved, right? It's hard to compare… If you got points for good karma, right, then there's probably more good karma in taking people off the streets supplying drugs to kids than there is preventing cyber-attacks! In terms of most personal fulfilment stuff, I found the private sector a new challenge and a different challenge and much more challenging and me having to evolve more than when I was with traditional law enforcement. (J54-60)

In contrast, Kate was less enthusiastic about her organisational identity and exhibited a preference for professional identity rather than organisational identity due to her experiences at her previous employer in the Intelligence community. The organisation experienced serious problems which, together with her frustrations, made her doubt the meaningfulness of her work as she could not see that her role contributed to the overall effort. This eroded her identification with the organisation and was the main reason Kate moved to the private sector. Her reliance on organisational identity for job satisfaction has reduced, making her more aware of her skills and the value she, in her profession, can bring to an organisation.

> The challenge was around feeling that as an individual, not me personally, it was across the board…it was as an individual, my role wasn't valued… We're putting a lot of time and energy into work that then just kind of got stuck in the spinning cycle. So it is important to me that I don't feel that my work will go out into the ether… in a vacuum. I don't have to feel like I'm saving lives every day… But there's some value… I should feel that there's value in my work overall or an opportunity to learn. (The situation at the Agency) … made me stronger professionally and personally… I needed to really figure out what I liked in the job, and I thought I was good at and what it wasn't. (K35-38)

Likewise, Vic has difficulty identifying with his employer due to the much narrower focus than when he served in the military. Previously, he felt that he served a greater good, but now, he finds it discouraging professionally to be in an organisation with a narrower purpose. This is why he is one of the participants who deliberately expanded his professional role and contribution to the broader organisation. He would not feel that he contributed to the organisation, thereby impacting his organisational identity.

> But unless I'm working with more of the broader organisation, I actually don't feel that I'm making a broader contribution because the internal clients I'm working with right now are quite focused; they're very narrow. I feel definitely… when I was an intelligence analyst in my former role, I did feel that… I was serving a greater good… and here I feel that I'm definitely serving not necessarily a lesser good, but just a much smaller and narrower purpose. So personally, for me, it's very discouraging professionally. (V36)

It is interesting to note how the participants with the strongest organisational identity are also those for have worked the longest for a specific company (Dave 20 years and Ben 9 years vis-à-vis Vic (7 years) and Kate and Josh (3 years). It seems as though there

is a direct correlation between the organisational identity, job satisfaction and retention of the participants. All three participants with a weaker organisational identity than Dave and Ben have moved to other companies since the interviews were conducted.

Subordinate theme 3.1(b): Values and behaviour

It is generally accepted that knowledge workers thrive in organisational circumstances where they are given the freedom or *autonomy* to perform their intellectually challenging work in a conducive context. Six of the ten participants shared how they appreciate the organisational culture where they are given free rein when "I was told to do what you think you should be doing."(J38)

For most of the participants, the autonomy that the organisation gave them was different from what they experienced in previous organisations, whether it was in the intelligence community or not. Now, they had the autonomy to identify and decide which issues they should focus on, talk to whomever they needed to get the job done and decide what resources they needed to do their job effectively and be creative. Josh summed it up succinctly when he stated that:

> There's a lot of freedom… there's a good amount of freedom in that you're asked to comment as you're the subject matter expert. You know the discipline. You determine what you should be looking at and how much effort and resources should be given to each other. I enjoy that freedom. (J77)

In the same vein, Dave valued the organisational culture of being open to other viewpoints where people have the freedom to differ from each other without consequences "the freedom to not agree with other views." (D36) Ben and Kate appreciated their organisational culture, where people are given the freedom to be entrepreneurial. Ben recounted an incident when he realised the extent of the latitude the organisation gave him when he discussed collection and analysis requirements with clients, and they turned the tables on him and said: "well, you're my analyst - tell me what they should be." (B28). Kate shared how she is now thriving in her company as she has ownership of her space as she is allowed to shape her function the way she sees fit and apply her networking skills to benefit the effort.

> I have ownership of my space, not a particular product. I have ownership over my space, and my space is asking questions, trying my best to figure this out, hold this puzzle together, get the information and then present it to someone. (K33)

This laissez-faire organisational culture can be counterproductive for SRIA as they need some kind of feedback or *validation* to ascertain whether they are fulfilling the organisation's needs. Ben shared how the lack of feedback from management initially made him think that they are not interested in what he has to say, but with time, he realised that they trust him enough to do his job and that he should not view their inattention negatively.

> I can't get regular time on their calendar to present to them… I'm a victim of my own success because I have a process that's working, and they're like, "well, that isn't on fire, that's not burning down. So I'm going to leave it alone and go focus on something else". (B31)

Participants shared how they would get validation from interaction with their counterparts in other organisations through functional networking, other colleagues and their interaction with fellow members of professional organisations. Those participants who are not members of professional organisations expressed that these networks could provide them with the validation they need to enact their professional identity.

However, there are also values and behaviour in organisations that disable the enactment of the participants' professional identity. Emma shared her frustration with the bank's organisational culture, where she works, as it does not afford her "space" to do what she wants to do. Even though she was the first risk intelligence analyst in the security department, the leadership had different ideas on what the role entails than her expectations. She ascribed these to a *critical and conservative mindset* that was mostly from her male colleagues who had a police background and, therefore, a different understanding of intelligence's function.

> My challenge is sometimes you come into the environment with different ideas trying to change how things are done. It takes a while to change behaviour. (E39) Some would try to block the good things it could implement; they are sabotaging you because of the mindset that I spoke about. (E62)

Similarly, a traditional and bureaucratic corporate culture where there is little innovation or an influx of outsiders bringing in new ideas is challenging for SRIA in the private sector. Kate's efforts to broaden the impact of her role to the broader company is stilted by the indifference of people who cannot understand the need for intelligence in their environments:

> There are parts of the business where people don't understand what I do, and they… it's an internal cultural thing. People aren't really mean or rude. The thing about my current company is that most of the people spent most of their career here. I have seen more interest by people who have had other professional experience and exposure to risk, and they would then ask me about intelligence and risk intelligence. But the others have a very narrow focus that is kind of limited. (K49)

Celia shared how surprised she was when she realised that the well-known consulting company she worked for did not espouse excellence and innovation. Their culture seemed to be doing just enough to deliver a service to clients, even if the service is mediocre. She resigned from the company because she could not agree with the pervasive satisficing attitude while trying to do everything with excellence.

> … Consulting companies… they don't really want to be excellent. You know good enough is good enough. You make more money when you just satisfy the need. You don't really... You almost never make more money by being excellent, you know, by exceeding expectations. And I found that very different to my own professional ethic. (C55)

Subordinate theme 3.1(c): Leadership

The way management embodies the organisational values and culture is decisive in whether the participants could effectively execute their roles and professional identity in the organisation. Positive relationships with leadership fostered a sense of support and belonging. Vic shared how his manager's accessibility and support fostered job satisfaction.

> I found it very helpful to have, for example, the head of security personally say to me, "You're doing a great job, or you're doing exactly what you should be doing"… He was actually very good at that in terms of support, and the other thing is the accessibility of senior management. He was also very accessible. He will talk to anybody from the registry clerk to the security officer, to you anytime.

Dave ascribed most of his success in the trust that his manager put in him 20 years before in the organisation. He allowed him to build up security risk management in the organisation, which expanded with time to become a dedicated protective intelligence function with a few spin-offs in other directions. His manager's leadership and the trust afforded to him contributed to his positive organisational identity.

However, negative relationships with leadership erode trust in the person as well as the organisation. Employees might be afraid to show initiative as it might be misconstrued, even regarded as threatening to the manager. This vicious cycle usually ends up being negative for both the people and the organisation. The most common negative relationship with management among the participants was their frustration that managers do not necessarily understand the role and function of intelligence in the private sector but are also not willing to learn and would therefore redirect the function, ignore it or sabotage it as seen with Emma's experience before.

It has been evident that Vic's relationship with his manager was healthy and provided him with the opportunity to contribute to the organisation to a larger extent. However, in subsequent personal correspondence after the interview, Vic shared how the company had some leadership upheaval, which led to the manager's departure. The organisational ecosystem disintegrated in the absence of a strong leader, and the employees felt that the issue was dealt with in an unprofessional manner that was not conducive to job satisfaction or collegiality. The new management team had a law enforcement background and focused on the physical security and investigations aspect rather than operational and strategic decision support. He decided to resign after it became clear that the new management did not support his role and did not heed his advice.

Subordinate theme 3.2: Organisational structure restraints impact

Some participants repeatedly stated that their function should not be based at the security department, especially those analysts who provide a knowledge service to other areas of the organisation. The main reason was that they felt that the lingering bureaucratic organisational culture is reinforced with their placement in the organigram,

although they provide a cross-sectional service fitting in a matrix or functional organisation design. To a large extent, this is based on how other people perceive them as part of the support function and not the core business of their organisations. Vic's deliberate efforts to disassociate himself with the security department has been discussed previously. Tina also shared her frustration with where her unit is placed in the security department:

> …the problem is actually being taken seriously and being misunderstood. So the role is misunderstood. Firstly are you a security guard? Are you an admin person? It's really never understood that you are fulfilling an intelligence analysis function. It's really misunderstood because of those things not having a professional body, but also not belonging to any other grouping within the institution. (T40)

Both she and Vic advocated that their function should rather be situated at a more strategic level where their output is company-wide and where the security department would be just one of their clients:

> I would want to sell intelligence to the bank. In the sense that intelligence should be a strategic output. (T62) and

> I'm also almost advocating for, you know, that there should be an intelligence office for the bank that's outside of security, and security should obviously be one of the main clients. (V113)

There are different types of functional models, wherever the structure itself is situated on the organigram. Andy and Kate, who have the widest reach in terms of internal clients, use external or embedded consultants or vendors such as Control Risks to provide general intelligence. Their task is then to contextualize it with their knowledge of the business needs and the operational and strategic requirements. Andy saw himself as the hub that gets the information from everywhere (including vendors) and then customise it to make it relevant to the client. Kate is concerned that both her external clients and companies, in general, would think that intelligence analysis is those products that vendors provide, without realising that someone still has to operationalise it and contextualise it for the company – asking the "so what for us?". She sees this as the greatest challenge for the profession.

> So I don't have to be, and none of my team has to be, a deep expert on Indonesia's electoral politics. We need to understand what the importance of elections in Indonesia is for our company… in what ways it

> could impact it and then find the experts to help us understand and then present and then we can take that information and contextualise and present it to our business. Our value is that we can understand our business really well and make all of that external vendor information relevant to this business. (K9-11)

Here, Kate has reinforced that the security risk intelligence analyst's main function is to provide insight and foresight about threat events and threat actors to the business, where they need it, and in the manner they need it. Here, the concept of the "right intelligence, at the right time, in the right format to the right person" is a timely reminder of what the profession should strive for. On a more pragmatic and realistic note, Ben admitted that security risk intelligence as a function would be a luxury for many organisations. He agreed that such a function is already illustrative of the sophistication of the organisation and the leadership's understanding that they need such a service.

> I think that SRIA is a luxury. In the traditional sense of like... you know if you can afford them, they provide value, but to really get the best out of people in that position, you have to have a fairly sophisticated …. You have to be either fairly far along in your own program, or they have to be able to take the initiative and be entrepreneurial. In the private sector, no one knows what you do. (A27)

Subordinate theme 3.3: Inappropriate HR practices

It is quite a daunting task to find someone with the right qualifications and attribute for a security risk intelligence analysis position. One of the refrains in the interviews is that analysts should be entrepreneurial to impact the organisation, which is a rare quality to find. At this stage, most participants have had bad experiences with Human Resources practitioners in the recruitment and staffing of positions in the field. It is acknowledged that HR practitioners should be guided by the recruiting manager for the typical processes related to establishing a post, the recruitment process and the retention of the individuals. As professionals in their own right, they should know what the job entails and the type of person who should be recruited. However, as discussed throughout this study, many people inside the organisation do not know the role and function of the security risk intelligence analyst.

The participants shared some of their experiences with inappropriate HR practices, especially recruitment. To a large extent, the recruiting managers are the culprits who

think, as Vic shared, “I can get anybody and they'll learn this job”. He experienced how people without the right qualifications, experience or attributes and skills were recruited in his organisation. These appointments eroded the morale and capability of the team as they had to be carried by the competent members of the group, while experienced members felt undervalued and overworked:

> I'm on a team of six, and four of the six have no post-secondary education; they have no relevant experience. For example, we have a human resources recruiter who was made into a senior Cybersecurity analyst and an executive administrative assistant made into a lead security analyst, and none of them has the right qualifications or experience. Those kinds of decisions erode the capability of the group… and they make those with experience bitter. It sounds personal, but it is very personal because you start to feel undervalued and you know you…, it's very basic to the human sort of instinct of feeling productive and saying, well, I worked hard for eight years to get to this position, where someone who hasn't, just gets it right? And we're being paid the same. (V75,76)

Celia also expressed her frustration with managers and HR personnel that would target certain veterans for the security risk intelligence analyst position, even if they have never performed the function before. The function then never reaches its full potential, while it could also have negative consequences for the company:

> …the company will hire the ex- FBI or Defence guy and ask them or expect them to be an analyst. And the ex-FBI security and the ex-Defence guy are so arrogant that they think they can do it. And it’s almost always a male, and the company gets terrible advice, right? But it is all kind of macho, golf club kind of stuff. You (as a woman) can't breakthrough. (C53)

Emma is dismissive about the recruitment process in her organisation as it seemed to her that the HR personnel uses proforma questions that have nothing to do with the outcomes required of the role.

> When we do interviews to recruit such people, we must refrain from having these downloaded questions on the internet… it does not bring value to the process of recruiting the right type of person for these posts. Even the psychometric tests – some of them will not give you what you’re looking for. For this specific career, something new has to be developed to attract people like that or to recruit people with a specific mindset I’m talking about. Most of the questions are, “Where do you see yourself in the next five years?” This has no relevance to a person’s job. (E35-37)

5.6 Discussion

This study aimed to develop an understanding of the experiences of SRIA in the private sector, including what it means to be in this profession and what factors impact their professional identity. The findings in Chapter 5 provide original insight into how they perceive their profession and develop strategies to overcome the many challenges they face when executing their role.

Their multi-faceted professional identity and the perceived impacts on professional relationships and the workplace have been highlighted. There are no other studies that empirically explored the professional identity of SRIA, whether they are in the private sector or the government sector, and therefore this study provides valuable insights into the lived experience of this group of under-researched professionals.

The use of IPA as an analytical method has proved valuable as it provided a detailed and rich description of the participant's lived experience. Figure 22 details the themes with each participant's relevant contributions. At times, the researcher was tempted to remove some of the participants' quotes as the word count increased. However, as this is the first study that gave a voice to the target group, it would have been sacrilege to do so. The key findings are reported against each superordinate and its subthemes.

THEMES	Andy	Ben	Celia	Dave	Emma	Josh	Kate	Lynn	Tina	Vic
Superordinate theme 1: Purposeful professional self										
1.1 Shared ideology of occupation										
1.1 (a) Role and function	O	O	O	O	O	O	O		O	O
1.1 (b) An analyst by any other name…	O			O		O	O			O
1.1 (c) Values guiding professional conduct	O	O	O	O	O		O			O
1.2 Multi-faceted professional self-concept										
1.2 (a) Pride in unique blend of skills and knowledge	O	O	O		O	O	O	O	O	O
1.2 (b) Personal attributes and attitudes	O		O	O	O		O	O	O	O
1.2 (c) Valence	O	O	O	O	O	O	O	O		O
1.3 Using professional identity tensions to grow										
1.3 (a) Impression management										O
1.3 (b) Job crafting and innovation	O	O			O		O	O	O	O
Superordinate theme 2: Connectedness to professional others										
2.1 A network rather than an association		O	O	O						O
2.2 "Prove that you are a business enabler"	O			O		O	O		O	
Superordinate theme 3: Enacting professional identity in the workplace										
3.1 Organisational culture is paramount										
3.1 (a) Organisational identity		O		O		O				O
3.1 (b) Values and behaviour		O	O	O	O	O	O			O
3.1 (c) Leadership		O	O							O
3.2 Organisational structure restraints impact	O	O				O	O		O	O
3.3 Inappropriate HR practices			O		O	O	O		O	O

Figure 22: Superordinate and subordinate themes with the relevant contributions of participants

5.6.1 Purposeful Professional Self

The participants revealed a deep-seated service orientation to protect and serve through two main objectives: 1) to provide expert advice on security threats and events that could impact the business and 2) provide risk intelligence support to decision-makers throughout the organisations. Only three of the ten focused primarily on the first objective of providing only security risk intelligence to clients. The majority of the participants (seven of the ten participants) have expanded their analytical and decision-support services and expertise to other functional departments in their organisations, enabling these stakeholders in procurement, marketing, distribution, and the like to make better decisions. On a personal level, some of the participants who have shown

their analytical mettle and understanding of the business are also roped into more strategic processes in the organisation, like strategic planning sessions.

It is clear from the interviews that the participants are not that much concerned about their job titles. They would rarely use their official job titles and would use whatever name would serve their purpose and audience in a specific context, even if it means that they would rather not say what they do, because it can lead to unwelcome questions. It seems as though what they do, matters more to them than what title is bestowed on them. The values of integrity and objectivity guide them in their professional lives, and it does not seem that any of them encountered major professional challenges that undermined those values. Only one participant shared that she resigned from the consulting company, where she worked as their mediocre deliverables and corporate culture clashed with her work ethics.

The results of their core competencies are aligned to Moore, Krizan, and Moore's (2005) three basic abilities necessary for intelligence analysis: thinking, collaborating and communicating. The participants' ability to think critically, creatively, on different levels of analysis and sensing the importance and relevance of events and information to business needs is the core of their abilities. As seen from the results, their competencies to communicate well to influence decision-making and liaise or collaborate with people to obtain and share information are critical to their role. What sets them apart from others, especially those in the intelligence community, is their application of these three core competencies in a business context. They need to understand the business of the organisation and identify who might be users of intelligence. The networking and client relationships become important to build trust relationships in which they foster a need for intelligence products and services and make sure they manage expectations effectively. SRIA in the private sector is a typical example of intelligence professionals that have changed their mind-set from a secretive "need to know" to a "need to share" and responsibility to provide" mind-set (Spracher, 2009).

The main attribute critical to a successful SRIA is a growth mindset in which they would welcome opportunities to learn and improve continuously as not one day is the same.

To counter-balance this excitement and quest for new information and insights, they also stressed the ability to be tenacious and patient. As Lynn stated, “it’s a slow-cooker, not MacDonald’s”, as it takes time to understand the complex problems one has to analyse, but also to build relationships that might influence operational and strategic decisions.

The participants exhibited positive feelings of job satisfaction and meaningfulness, mainly since they can use their skills in an environment that espouses innovation and entrepreneurial thinking to benefit the organisation. This finding supports Mercurio (2019) that a positive attitude to work, the enacting of personal values, having pride in one’s skills and knowledge and developing positive relationships make work meaningful. There were no negative feelings towards their personal experience as SRIA in the private sector. The only negative aspects were in an organisational context related to the external perception of the security department and lingering racial and gender biases in organisations. The participants applied both main identity work strategies. Vic only applied identity protection strategies (impression management and disassociation). All participants used identity restructuring strategies to extend their role content through job crafting and innovation to overcome a perceived lack of legitimacy and extend their influence in the company.

5.6.2 Connectedness to others in a professional context

Their connectedness with others in the workplace had two main objectives: firstly, to strengthen their understanding of the subject matter, they have to research and to seek validation from peers in functional networks, social media and mentoring while, secondly, to gain understanding and acceptance with stakeholders to see them as valuable partners in achieving business objectives. Both these objectives serve their professional identity quest well, as it forces them to be self-aware of their shortcomings and think about ways to satisfy new stakeholders’ intelligence needs through pragmatic and persuasive relationships. Membership of professional organisations is not of paramount importance to them as their individual professional identity is strong, and they experience validation in their professional networking. The disassociation from or

disinterest in professional organisation membership is not necessarily a negative reflection on professional organisations. Rather, it should be seen that SRIA's are rather "lone than pack animals" and would seek out professional organisations if they think it could be to their benefit.

5.6.3 Professional Identity Enactment in the Workplace

The workplace as structure is both an enabler and disabler of professional identity enactment. As the participants mainly find meaningfulness in their work in their ability to use their skills and knowledge, the organisational identity was not a critical factor in their professional identity enactment. Companies with values reflecting a society-wide mission and responsibility positively correlated to the participants' expression of meaningfulness in making a difference and protecting or serving something greater than themselves. These three participants' organisational identity was relatively strong, while the rest did not rate this factor high when discussing how the organisational context influences their professional identity.

The most prominent organisational culture factor that enabled professional identity is autonomy and a value of excellence to perform their role to the best of their ability. On the flip side, this would also mean that there might not be sufficient validation of work done. To counter this ambivalence, effective leadership has proved to be critical in ensuring that the participants retain their focus and enthusiasm.

Not many organisations have evolved into a matrix networked organisational structure and remained in the Tayloristic bureaucratic stance, leading to at least one participant struggling professionally. For the others, the organisational placement of their analytic function within the security department had implications in terms of impact and power relations. It is difficult to counter the perception that the security department is a stepchild to the core business and made-up of "mall cops" and convince people that you are a highly qualified and experienced knowledge worker who can offer a force-multiplier service. The participants offer some suggestions on which business model could work best to address this current workplace problem.

Lastly, unsuitable Human Resources practices disabled the participants' enactment of their professional identity in the workplace due to incorrect recruitment practices and the absence of career pathing. This led to poor retention rates, job dissatisfaction and disengagement, but worse, it entrenched a practice that is damaging to the career group as a whole. Proposals for the improvement of these practices will be made in the last chapter.

5.7 Limitations

The principle of credibility is critical when assessing a qualitative study like this, especially using IPA as a method. The researcher's main motivation for using IPA was to give a voice to the participants. One of the study's main limitations was the impact of language, as the researcher and three of the participants were not first-language English speakers. Often, the meaning of the idioms and terminology could have been interpreted differently, but the researcher attempted to accept the intended meaning of the transcripts in the context of the questions and how the interview took place.

Although a strength for this study is that there was a broad representation of different organisational contexts in which the participants worked, it was also a limitation. There were unique organisational contextual factors that may have influenced the participants' responses without the researcher being aware of these.

Another limitation was time constraints that prevented the researcher from interviewing participants a second time to clarify certain issues that emerged during the first phase of interpretation. Some dimensions "screamed" screamed for further discussion, or even maybe a longitudinal approach to determine whether there was any growth or change in the participants' sense-making in certain aspects, like meaningfulness in the workplace.

5.8 Conclusion

This chapter discussed the professional identity of individual SRIA in the private sector, using IPA as a qualitative method to obtain rich and granular data. The study concluded that the professional identity of individual security risk intelligence analysts in the

private sector is similar across the five countries and the different organisational contexts that were represented.

The study concluded that they perceive to play an important role in securing their companies and society in the broader sense. Their professional identity is centred on their expert knowledge and ability to perform complex intellectual tasks in providing forewarning and insight into threats to the organisation or client's well-being and sustainability. They are generally people with a strong individual professional identity that reflects high levels of job satisfaction, pride and autonomy in their profession who thrive on connecting on a professional, functional level with stakeholders. Their main professional challenge related to the relative lack of understanding of their role in the private sector by the HR department and potential clients of their deliverables. Those who are entrepreneurially inclined and wanted to extend their impact on the organisation—as they feel they can make a greater contribution—are frustrated that there is not better acceptance due to this unfamiliarity.

Chapter 6

Integrated analysis

6.1 Introduction

This chapter will summarise and integrate the findings of the two empirical studies and literature in relation to the research objectives and questions presented in the thesis with the implications for praxis. Some suggestions are made for further research.

6.2 Discussion of findings in relation to the context of the research questions

The findings of the research confirm Ashforth's (2016) notion that "identity bridges all levels of analysis, levels of self, and a multitude of disciplines" that brought about "exciting and important" research results on the professional identity of security risk intelligence analysts in the private sector. The three main research objectives were adequately investigated, and credible findings were made.

6.2.1 Does an emerging profession exist in the security risk intelligence discipline for analysts on an international level?

The participation of 75 respondents in Study 1 (16 different nationalities, working in 28 countries with three working globally) and 10 participants from five different countries who participated in the second study, confirmed that there are people who self-identified and associated themselves with the profession.

6.2.2 What is the professional identity of the individual Security Risk Intelligence Analyst in the private sector?

Although the profession is relatively new, and the participants were from diverse types of organisations, economic sectors and countries, the findings offer a surprisingly similar or shared professional identity. The results indicate that the construct of Social Identity Theory (SIT) of Tajfel and Turner (2004) and Turner's Self-Categorisation Theory (SCT) is applicable in the context of the thesis. Analysts have shown that, individually, they

identify themselves with a perceived group of people who perform the same professional functions by participating in the study.

This means that people have wilfully decided that there exists such a profession as *Security Risk Intelligence Analysis*, even though they might not necessarily have had interactions with such a group or belonged to professional organisations that serve the group (Brooks et al., 2011). One of the contributions of this study might be that people realise that there is such a profession that they can identify with. For the first time, individuals could externalise their identification and association with the core (this is me), content (I am like) and behaviours (I act like one) of the professional group (Ashforth et al., 2008). Therefore, their individual professional identity became the blueprint of the collective professional identity that will be discussed in the next section. There were some elements of difference, but none of them impacted the overall convergence of perceptions that emerged during the study. These differences could be ascribed to the main characteristics of professional identity: it is multifaceted, dynamic, have individual agency, and changes in interaction with others. The differences, therefore, contributed to the richness and thickness of the data, while it also opened up opportunities for further research.

6.2.3 Is there a shared or collective professional identity among Security Risk Intelligence Analyst in the private sector?

The findings prove that there is indeed a collective professional identity among the participants in the target group as the seven prerequisites (Ashmore et al., 2004) of "self-categorisation that is shared with a group of others" have been met as discussed below:

i) SRIA self-categorise with the profession

Individual SRIA placed themselves in the professional group when they participated in the study as they perceived themselves to be similar in one way or the other with the group. The criteria for participation in the study were extensive and served as preconditions of not only participation in the study, but also a pre-emptive expression of belongingness to the emerging profession.

SRIA also feel that they offer something unique to the work ecology that no other profession does. Whether this is actually true or not is irrelevant as this is how they subjectively make sense and articulate their professional identity in their quest to find ways to contribute meaningfully to society.

ii) SRIA have positive (and negative) attitudes towards the profession (evaluation)

The shared values of integrity, honesty, and objectivity that most participants offer are typical of many professions and not unique to security risk intelligence analysis. The vast majority of the participants have a good perception of their profession and would recommend the job to other people with the same interests and skills. The only negative attitudes related to the contra points of the positive aspects. In this sense, a major concern might be that SRIA can become frustrated due to a notion that they can do so much more than what the organisation allows them to do or do not have sufficient resources or that HR practices impede them. This could lead to burn-out, especially where the intellectual inputs that the role requires, or feelings of frustrations, does not match personal expectations and organisational realities.

iii) The degree of importance of group membership to the individual's overall self-concept

Due to the idiosyncrasies of individual context and personal interests, the findings did not prove an overwhelming shared benefit from belonging to this profession. However, the simple majority (51%) value the intellectually stimulating nature of the work and the self-validation and respect they derive from executing this role. Job satisfaction is closely related to identifying with the organisations' values and an organisational culture that allows autonomy and growth opportunities. They would primarily identify with the profession for personal reasons: to exploit or gain a better understanding of the subject matter and, more importantly, because they get validation from peers when they can share their advanced thinking skills and expert deliverables. Some of them might also associate with the profession to gain knowledge about best practice and benchmark to improve their own professional processes.

iv) The affective sense of belonging or attachment and sense of interdependence with the social group

They see themselves as a valuable partner in protecting the private sector's interests, including their employees, clients, processes and products or services. However, at this stage, the affective sense of belonging is definitely grounded in the individual benefit and esoteric value they think they bring to the workplace and not in a common feeling of attachment to the wider group. The interdependence level is low, and there is no evidence of feeling ashamed when someone in the same role in another context or company does something wrong. They do not see it as bringing disrepute to the profession. The main reason for this might be that this is really an emerging profession and that the sense of belonging has only just manifested and is therefore still very much in the I/me phase.

v) The degree to which the individual is socially embedded with a particular collective identity

One of the more interesting findings of the study is that self-identification with the profession does *not* rely on social interaction (Ashforth & Mael, 1989) and is therefore *not* an indicator of or a prerequisite for a strong professional identity. Although most of the survey participants belonged to professional organisations, only 14 (19%) belonged to a body specifically aimed at security risk intelligence analysts (AIRIP). Functional interaction and liaison seem to be preferred above the social interaction, networking and related sharing of best practices in the context of a professional organisation.

vi) The extent of behavioural involvement with the social group

The study confirmed that the SRIA shared the same behaviour (what we do) with others in the profession. Their role and function were very clear as being "providing forewarning and situational awareness". This rhetoric also strengthens their professional identity because it is seen as the essence of their trade, resulting in a mutually beneficial relationship where the more they use rhetoric, the stronger their professional identity becomes.

vii) The content and meaning the collective identity provides to the individual in terms of the extent to which the individual associates self-descriptive characteristics with the group, the group's ideology and group narrative or history.

As this profession is emerging, there would be little to share in history and ideology, even self-descriptions. The most common refrain among the participants in both studies was that their role and function are not known in the organisation or among the general public. Therefore, it is not easy to offer a value proposition to the business beyond the security department. This should not pose too much of a problem with companies and professionals who already have well-established intelligence analysis units in their security departments. However, many of the participants exhibited an entrepreneurial spirit in which they would like to expand their value proposition to "more than just security". The unfamiliarity with their function might prove to be too difficult to overcome, especially in more bureaucratically inclined organisations or where the placement of such a function can prove difficult to manage in terms of the power dynamics. However, this venture could be attainable in companies that are already moving towards a matrix-based organisation where the function could be appreciated and used to achieve multiple organisational objectives.

Ironically, the fact that the participants do not share a common job title, or even a job description, is a shared characteristic. This would imply that the title is not as important as the work and value one offers to your stakeholders. The one consequence of this absence of shared job titles is that they have an individualised outlook on their professional identity. They would rather be known by their names than by their titles, which might also be typical of a new breed of knowledge workers in the current individualistic society.

6.3 Limitations

The limitations of the two empirical studies were discussed in previous chapters, but the two overarching limitations of the thesis will be discussed here. The first overall possible limitation was the generalisability of the findings as the actual target population's size is not known. There is no way to determine whether the 75 participants in the survey, of which ten then participated in the interviews, is fully representative of the SRIA

professional community. The second possible general limitation was that the researcher's subjectivity and insider experience might have influenced the validity of the findings. The fallible human element has been present throughout the research: from the development of the two research instruments, the interview process, the coding and identification of themes and the interpretation of the data.

6.4 Contribution to the Security Risk Management field

This study makes three contributions to the Security Risk Management discipline. Firstly, it provides an evidence base to inform industry, education and professional organisations on the typical profile and functions of the emergent profession of SRIA. Secondly, it contributes to an understanding of how the different dimensions of professional identity shape these professionals and their search for professional meaningfulness. Lastly, the study also makes four main recommendations to SRIA and other stakeholders to strengthen the development of the profession and the identity of the practitioners in this emerging field.

6.5 Recommendations and further research

Four broad recommendations are made to SRIA, their managers, professional bodies, Human Resources practitioners dealing with these professionals, and other stakeholders in the private security sector.

6.5.1 Create opportunities to reflect on professional identity and meaningfulness

All the participants in the study commented that this was the first opportunity they ever had to reflect on their work and the reasons they chose to remain in this profession. Usually, individuals and organisations blame a lack of time and opportunity as reasons why reflection and learning opportunities are not actively encouraged. The value of mindfulness or self-awareness is critical to job satisfaction and effectiveness. In this regard, it would be helpful to regularly reflect on one's professional objectives, whether there is a synergy between personal and organisational values and identify ways to maximise one's impact on the workplace (see Appendix E for a proposed worksheet that could be used for professional reflection).

Professional organisations or analytical units in organisations could also use the questions posed in the survey and interviews and those in Appendix E to enable sessions during which analysts could externalise their professional identity and professional needs, thereby discovering commonalities and strengthening collective professional identity. Some of the resultant benefits could be that professional organisations would better understand why analysts become members of, or steer away from professional organisations, thereby ensuring that they offer the benefits that SRIA requires in a collective professional context.

As this was the first study in the professional identity of SRIA in the private sector, it might be useful to conduct longitudinal studies to determine changes in the professional identity factors identified in this study. Pointers might include the demography of analysts and to what extent younger analysts find a professional home in the industry, whether the demand for SRIA has increased or decreased in the private security sector and to make proposals for a viable professional pipeline to ensure the strengthening and growth of the profession in the future.

6.5.2 Define the unique value proposition of SRIA to stakeholders

It is clear from the research findings that few of the stakeholders understand the function of SRIA and its value to the private sector. It is crucial that prominent SRIA and professional organisations in the security or risk domain, like AIRIP and ASIS, advocate awareness of the function and its value to security and other organisations focusing on protective risk. These awareness campaigns can be launched across digital and physical channels to reach all stakeholders, including business media outlets, conferences, television and radio, podcasts, and all other stakeholders' communication channels.

To support these advocacy campaigns, research can be done in a typical business school context regarding stakeholder analysis, Return on Investment (ROI) driver analysis, and the different business models in which the SRIA function creates value to organisations. This study identified a range of business models, including in-house experts, embedded consultants, matrix cross-functional expert advisers and different levels of outsourced variants.

It is further recommended that SRIA engage with their managers and HR partners to relook the job title and description to reflect the actual functions and responsibilities of SRIA in the private sector.

6.5.3 Partner with organisational Human Resources and professional HR bodies to improve HR practices in Security Risk Management

To bolster the recognition of SRIA and address the identified challenges with inappropriate Human Resources practices, it is prudent that individual SRIA make an effort to educate their hiring and HR managers on the role, functions and requirements of the function. On a broader, more strategic level, companies and professional bodies, like AIRIP and ASIS, could partner with relevant Human Resources bodies that develop a systematic classification of job roles and required skillsets for this emerging profession. The results can support business leaders and HR managers in establishing clear strategies for recruiting and developing the right skills needed to leverage security risk Intelligence analysis in the workplace. It can also help establish a common vocabulary to be used by HR recruiters and education providers so that supply and demand can more effectively meet in the job marketplace. Another benefit would be the definition of appropriate career pathways and retention strategies for this professional group.

6.5.4 Make the SRIA profession future-ready by exploiting synergies in related sectors such as cybersecurity, data science, business continuity management and resilience

This study identified those skills and competencies that would be critical for SRIA to remain relevant in a world where threats are increasingly multidimensional, interconnected and manifesting in the cyber domain. Analysts would need to be trained in dark web exploitation, data visualisation, coding, data science, and artificial and augmented intelligence to create real-time response algorithms to identify vulnerabilities and build scenarios to conduct strategic threat futures.

The critical thinking, analytical and communication skills of SRIA should not only be restricted to the security management and risk disciplines. These skills are high in demand, and researchers could identify and develop shared interests and transversal

skills in emerging technology-related fields. This might mean that the SRIA expand their impact to a wider field and even create new career opportunities away from the security risk discipline. One example is “data interpretation” or “analytics translation” which has created a niche for people with these skills to connect technical data scientists with the business needs and objectives.

6.6 Conclusion

The present study highlighted the importance of a well-developed and strong professional identity of security risk intelligence analysts in the private sector. The research illustrated how a weak or absent professional identity in the security context could inhibit individual professional growth and job satisfaction. This could lead to losses, harm to employees, customers or the general public and reputational damage to the company. The study concluded that there are indeed practitioners across the world and organisational contexts who self-identify with a “security risk intelligence analyst” profession. Furthermore, they share a professional identity that is more based on individual excellence, intellectual labour, networking and pragmatic relationship management than a group-based broad self-concept.

Bibliography

Aangenendt, M.T.A. (2015). Understanding changes in employees' identification and professional identity: the case of teachers in higher vocational education in the Netherlands. (Doctoral thesis). University of Twente, Netherlands.

Aangenendt, M.T.A., Kuijpers, M., & Sanders, K. (2012). Professional identity of teachers in higher professional education: a qualitative case study. In *Dialogue Do! Sustainable professionalization in higher professional education,* 145-172. The Hague: The Hague University of Applied Sciences, Center for Lectorates and Research. ISBN: 978-90-73077-38-6

Aangenendt, M.T.A., Neelen, G., Willems, P., & Lavèn, I. (2018). Professionals alike and unlike: A tool for dialogue on the professional diversity of lecturers and researchers in higher vocational education. In Frans Jacobs & Ellen Sjoer (Eds.). *Inspired to change: A kaleidoscope of transitions in higher education.* 38-51. ISBN: 978-90-73077-94-2

Alase, A. (2017). The Interpretative Phenomenological Analysis (IPA): a guide to a good qualitative research approach. *International Journal of Education and Literacy Studies, 5*(2), 9-19. http://dx.doi.org/10.7575/aiac.ijels.v.5n.2p.9

Aldridge, M., & Evetts, J. (2003). Rethinking the concept of professionalism: the case of journalism. *The British Journal of Sociology*, *54*(4), 547-564. Retrieved from https://europepmc.org/article/med/14660258

Alves, S., & Gazzola, N. (2011). Professional identity : A qualitative inquiry of experienced counsellors. *Canadian Journal of Counselling and Psychotherapy, 45*(3), 189-207. Retrieved from https://eric.ed.gov/?id=EJ944808

Alves, S., & Gazzola, N. (2013). Perceived professional identity among experienced Canadian counsellors: A qualitative investigation. *International Journal for the Advancement of Counselling, 35*(4), 298-316. https://doi.org/10.1007/s10447-013-9184-x

Alvesson, M. (2001). Knowledge work: Ambiguity, image and identity. *Human Relations, 54*(7), 863–886. https://doi.org/10.1177/0018726701547004

Alvesson, M. (2011). De-essentializing the knowledge intensive firm: Reflections on sceptical research going against the mainstream. *Journal of Management Studies, 48*(7), 1640-1661. https://doi.org/10.1111/j.1467-6486.2011.01025.x

Alvesson, M., Ashcraft, K. L., & Thomas, R. (2008). Identity matters: Reflections on the construction of identity scholarship in organization studies. *Organization, 15*(1), 5-28. https://doi.org/10.1177/1350508407084426

Ashforth, B. E. (2016). Distinguished scholar invited essay: Exploring identity and identification in organizations: Time for some course corrections. *Journal of Leadership & Organizational Studies*, *23*(4), 361-373. https://doi.org/10.1177/1548051816667897

Ashforth, B. E., Harrison, S. H., & Corley, K. G. (2008). Identification in organizations: an examination of four fundamental questions. *Journal of Management, 34*(3), 325-374. https://doi.org/10.1177/0149206308316059

Ashforth, B. E., & Mael, F. (1989). Social identity theory and the organization. *Academy of Management Review, 14*(1), 20-39. Retrieved from http://www.jstor.org/stable/258189

Ashmore, R. D., Deaux, K., & McLaughlin-Volpe, T. (2004). An organizing framework for collective identity: Articulation and significance of multidimensionality. *Psychological Bulletin, 130*(1), 80-114. https://doi.org/10.1037/0033-2909.130.1.80

Association of International Risk Intelligence Professionals (AIRIP). (2015). *AIRIP Code of Conduct*. Retrieved from https://www.airip.org/page/standards_guidelines

Babbie, E. (2015). *The practice of social research* (14th ed.). Boston: Wadsworth Cengage Learning. ISBN:1305445562, 9781305445567

Ball, N., Biesheuvel, P., Hamilton-Baillie, T., & Olonisakin, 'Funni. (2007). *Security and justice sector reform programming in Africa* (Evaluation Working Paper 23). Retrieved from https://www.oecd.org/countries/sierraleone/38635081.pdf

Bar-Joseph, U. (2011) The professional ethics of intelligence analysis. *International Journal of Intelligence and CounterIntelligence*, *24*(1), 22-43. https://doi.org/10.1080/08850607.2011.519222

Bayerl, P. S., Horton, K. E., & Jacobs, G. (2018). How do we describe our professional selves? Investigating collective identity configurations across professions. *Journal of Vocational Behavior, 107*, 168-181. https://doi.org/10.1016/j.jvb.2018.04.006

Bazeley, P. (2015). Computer-assisted integration of mixed methods data sources and analyses. In A. Tashakorri & C. Teddlie (Eds.) *SAGE handbook of mixed methods in social & behavioral research*. https://doi.org/10.4135/9781506335193

Bean, H. (2015). Privatizing intelligence. In R. Abrahamsen & A. Leander (Eds.), *Routledge handbook of private security studies*. Routledge.

Becker, L. A. (2020). The right stuff: an interpretive phenomenological analysis of NASA safety & mission assurance leaders making sense of their professional identity. (Doctoral thesis). Northeastern University, Boston, MA. Retrieved from https://repository.library.northeastern.edu/files/neu:m045qf58f/fulltext.pdf

Beech, N., Macintosh, R., & Mcinnes, P. (2008). Identity work: processes and dynamics of identity formations. *International Journal of Public Administration 31*(9). Retrieved from https://eprints.gla.ac.uk/24581/1/24581.pdf

Beijaard, D., Meijer, P. C., & Verloop, N. (2004). Reconsidering research on teachers' professional identity. *Teaching and Teacher Education*, *20*(2), 107-128. https://doi.org/10.1016/j.tate.2003.07.001

Bersin, J. (2017). Catch the wave: The 21st-century career. *Deloitte Review*, *(21)*, 62-79. Retrieved from

https://www2.deloitte.com/content/dam/insights/us/articles/3943_Catch-the-wave/DUP_Catch-the-wave-reprint.pdf

Bévort, F., & Suddaby, R. (2016). Scripting professional identities: how individuals make sense of contradictory institutional logics. *Journal of Professions and Organization, 3*(1), 17-38. https://doi.org/10.1093/jpo/jov007

Bielska, A., & Pallaris, C. (2017). *Redefining the intelligence skill set through the prism of the intelligence analysis impact model.* Retrieved from https://www.yumpu.com/en/document/read/57315016/2n3g1wg

Biesta, G. (2010). Pragmatism and the philosophical foundations of mixed methods research. In A. Tashakorri & C. Teddlie (Eds.), *SAGE handbook of mixed methods in social & behavioral research*, 95-118. https://dx.doi.org/10.4135/9781506335193.n4

Bode, R. (2016). What does a Risk Intelligence Analyst do? [Blog post]. Retrieved from http://www.airip.org/members/blog_search.asp?t=1&q=WhatDoesARiskIntelligenceAnalystDo

Booysen, L. A. E. (2018). Workplace identity construction: an intersectional-identity-cultural lens. In *Oxford research encyclopedia of business and management*. https://doi.org/10.1093/acrefore/9780190224851.013.47

Brandis, S., Fitzgerald, A., Avery, M., McPhail, R., Fisher, R., & Booth, J. (2016). The emergence of new kinds of professional work within the health sector. In *Perspectives on contemporary professional work*. Cheltenham, UK: Edward Elgar Publishing. DOI: https://doi.org/10.4337/9781783475582.00021

Brannen, J. (2005). *Mixed methods research: A discussion paper*. (Economic And Social Research Council National Centre for Research Methods, NCRM Methods Review Papers, NCRM/005). Retrieved from http://eprints.ncrm.ac.uk/89/

Briggs, A. R. J. (2007). Exploring professional identities: Middle leadership in further education colleges. *School Leadership and Management, 27*(5), 471-485. https://doi.org/10.1080/13632430701606152

Brooks, N. G., Riemenschneider, C. K., Hardgrave, B. C., & O'Leary-Kelly, A. M. (2011). IT professional identity: Needs, perceptions, and belonging. *European Journal of Information Systems, 20*(1), 87-102. https://doi.org/10.1057/ejis.2010.48

Brott, P. E., & Myers, J. E. (1999). Development of professional school councelor identity: A grounded theory. *Professional School Counseling, 2*(5). Retrieved from https://libres.uncg.edu/ir/uncg/f/j_myers_development_1999.pdf

Brouard, F., Bujaki, M., Durocher, S., & Neilson, L. C. (2017). Professional accountants' identity formation: an integrative framework. *Journal of Business Ethics, 142*(2), 225-238. https://doi.org/10.1007/s10551-016-3157-z

Brown, Z. T. (2019). *Intelligence's accidental profession*. Retrieved from Real Clear Defence website: https://www.realcleardefense.com/articles/2019/08/20/intelligences_accidental_profession_114679.html

Burns, S., & Cruikshanks, D. R. (2017). Evaluating independently licensed counsellors' articulation of professional identity using structural coding. *The Professional Counselor, 7*(2), 185-207. https://doi.org/10.15241/sb.7.2.185

Butler, N., Chillas, S., & Muhr, S. L. (2009). Professions at the margins. *ephemera, 9*(2), 78-194. Retrieved from https://www.academia.edu/10165905/Professions_at_the_Margins

Byrnes, N. (2017). *As Goldman embraces automation, even the masters of the universe are threatened*. Retrieved from MIT Technology Review website: https://www.technologyreview.com/2017/02/07/154141/as-goldman-embraces-automation-even-the-masters-of-the-universe-are-threatened/

Cardoso, I., Batista, P., & Graça, A. (2014). Professional identity in analysis: a systematic review of the literature. *The Open Sports Sciences Journal, 7*(1), 83-97. https://doi.org/10.2174/1875399X01407010083

Caza, B. B., & Creary, S. J. (2016). The construction of professional identity. In Adrian Wilkinson, D. Hislop, & C. Coupland (Eds.), *Perspectives on contemporary professional work: Challenges and experiences*, 259-285. Cheltenham, UK: Edward Elgar Publishing. Retrieved from http://scholarship.sha.cornell.edu/articles/878

Caza, B. B., Vough, H., & Puranik, H. (2018). Identity work in organizations and occupations: Definitions, theories, and pathways forward. *Journal of Organizational Behavior, (39)* 889- 910. https://doi.org/10.1002/job.2318

Cobbold, C. (2015). Professionals without a profession? The paradox of contradiction about teaching as a profession in Ghana. *Journal of Education and Practice, 6*(6), 125-134. Retrieved from https://files.eric.ed.gov/fulltext/EJ1083583.pdf

Corvaja, A. S., Jeraj, B., & Borghoff, U. M. (2016). The rise of intelligence studies: a model for Germany?. *Connections*, *15*(1), 79-106. Retrieved from https://procon.bg/system/files/15.1.06_intel_studies.pdf

Costas, J., & Kärreman, D. (2016). The bored self in knowledge work. *Human Relations, 69*(1), 61-83. https://doi.org/10.1177/0018726715579736

Cowin, L. S., Johnson, M., Wilson, I., & Borgese, K. (2013). The psychometric properties of five professional identity measures in a sample of nursing students. *Nurse Education Today 33*(6), 608-613. Retrieved from https://ro.uow.edu.au/cgi/viewcontent.cgi?article=1934&context=smhpapers

Cranitch, K. (2017). *Professional identity: shaping attraction, retention, and training intentions in early childhood education and care*. (Doctoral dissertation). Queensland University of Technology, Australia. Retrieved from https://eprints.qut.edu.au/112813/2/Christina_Cranitch_Thesis.pdf

Creswell, J. W. (2009). *Research design: qualitative, quantitative and mixed-method approaches,* 203-223. SAGE Publications, Inc. Retrieved from http://www.drbrambedkarcollege.ac.in/sites/default/files/research-design-ceil.pdf

Crump, J. (2015). *Corporate security intelligence and strategic decision making*. CRC Press. https://doi.org/10.1201/b18399

Dorough-Lewis, J. (2017). *Exploring identity and negotiation among women military interrogators through Interpretative Phenomenological Analysis*.(Doctoral dissertation). Nova Southeastern University, Florida, US. Retrieved from https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1053&context=shss_dcar_etd/

Duvenage, M. A. (2010). *Intelligence analysis in the Knowledge Age: An analysis of the challenges facing the practice of intelligence analysis* (Unpublished masters thesis). Stellenbosch University, South Africa. Retrieved from https://scholar.sun.ac.za/handle/10019.1/3087

Dvojmoč, M. (2019). Corporate Intelligence as the New Reality: The Necessity of Corporate Security in Modern Global Business. *Journal of Criminal Justice and Security*, (2), 205-223. Retrieved from https://www.fvv.um.si/rV/arhiv/2019-2/06_Dvojmoc_rV_2019-2.pdf

Dynes, J. (2014). Professionalism and practice: the development of situational vocational professional identity amongst UK Army Reserve instructors. (Doctoral dissertation). University of Brighton, UK. Retrieved from https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.649361

Eatough, V., & Smith, J. A. (2017). Interpretative phenomenological analysis. In C. Willig & W. Stainton-Rogers (Eds.), *Handbook of Qualitative Research in Psychology* (2nd ed). 193-209. Sage Publications. https://doi.org/http://dx.doi.org/10.4135/9781526405555

Elvey, R., Hassell, K., & Hall, J. (2013). Who do you think you are? Pharmacists' perceptions of their professional identity. *International Journal of Pharmacy Practice*, *(21)* 322-332. https://doi.org/10.1111/ijpp.12019

Evetts, J. (2011). Sociological analysis of professionalism: Past, present and future. *Comparative Sociology, 10*(1), 1-37. https://doi.org/10.1163/156913310X522633

Feilzer, M. Y. (2010). Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of Mixed Methods Research, 4*(1), 6-16. https://doi.org/10.1177/1558689809349691

Ferrucci, P., & Vos, T. (2017). Who's in, Who's out?: Constructing the identity of digital journalists. *Digital Journalism, 5*(7), 868-883. https://doi.org/10.1080/21670811.2016.1208054

Fisher, L. D. (2017). *Registered counsellors at a crossroads: Current status, professional identity and training realities.* (Doctoral dissertation). Stellenbosch University, South Africa. Retrieved from http://scholar.sun.ac.za/handle/10019.1/102980

Franke, V., & Von Boemcken, M. (2009). Private guns: the social identity of security contractors. *Journal of Conflict Studies*. *29*, 118-131. Retrieved from https://journals.lib.unb.ca/index.php/JCS/article/view/15237/24497

Fraser-Arnott, M. A. (2017). Personalizing professionalism: The professional identity experiences of LIS graduates in non-library roles. *Journal of Librarianship and Information Science, 1*(9). https://doi.org/10.1177/0961000617709062

Fraser-Arnott, M. A. (2019). Evolving practices and professional identity: How the new ways we work can reshape us as professionals and a profession. *IFLA Journal*, *45*(2), 114-126. https://doi.org/10.1177/0340035218810960

Gazzola, N., & Smith, J. D. (2007). Who do we think we are? A survey of counsellors in Canada. *International Journal for the Advancement of Counselling, 29*(2), 97-110. https://doi.org/10.1007/s10447-007-9032-y

Gill, M. (2015). Elite identity and status anxiety: An interpretative phenomenological analysis of management consultants. *Organization, 22*(3), 306-325. https://doi.org/10.1177/1350508413514287

Goertzen, M. (2018). The professional identity experiences of LIS graduates in non-library roles can be described by the theory of personalizing professionalism. *Evidence Based Library and Information Practice*, *13*(1), 21-23. https://doi.org/10.18438/eblip29356

Gray, D. E. (2011). Journeys towards the professionalisation of coaching: dilemmas, dialogues and decisions along the global pathway. *An International Journal of Theory, Research and Practice*, *4*(1), 4-19. https://doi.org/10.1080/17521882.2010.550896

Gray, D. E. (2014). Theoretical perspectives and research methodologies. In *Doing research in the real world*. Sage. Retrieved from https://in.sagepub.com/sites/default/files/upm-binaries/58626_Gray__Doing_Research_in_the_Real_World.pdf

Gray, D. E., Saunders, M., Curnow, B., & Farrant, C. (2015). Coaching: An emerging profession – or just a spanner in the HRD toolbox? In *The 16th International Conference on Human Resource Development Research and Practice across Europe: UFHRD*. Retrieved from https://www.ufhrd.co.uk/wordpress/wp-content/uploads/2015/09/Coaching-An-emerging-profession-%E2%80%93-or-just-a-spanner-in-the-HRD-toolbox.docx

Groth, T. M. (2015). Using the collective identity construct to examine the role of a farmer occupational identity in multi-functional landscapes in Australia and the United States. (Unpublished doctoral thesis). Charles Sturt University, Australia. Retrieved from https://researchoutput.csu.edu.au/files/9316320/82193

Grubenmann, S., & Meckel, M. (2014). Metaphors of occupational identity: Traces of a changeable workplace in journalism. *Academy of Management Proceedings*, 1-41. Retrieved from https://www.alexandria.unisg.ch/230705/1/Metaphors%20of%20Occupational%20Identity.pdf

Hare, N., & Coghill, P. (2016). The future of the intelligence analysis task. *Intelligence and National Security, 31*(6), 858-870. https://doi.org/10.1080/02684527.2015.1115238

Harwood, N. (2017). *Exploring professional identity: a study of American sign language/English interpreters.* (Master's thesis). Western Oregon University, Monmouth, Oregon. Retrieved from https://digitalcommons.wou.edu/theses/37/

Haslam, S. A. (2004). *Psychology in organizations: The social identity approach*, 17-39. London: SAGE Publications Ltd. https://doi.org/10.4135/9781446278819

Herbert, M. (2013). The motley of intelligence analysis : getting over the idea of a professional model. *International Journal of Intelligence and Counterintelligence, 26*(4), 652-665. https://doi.org/10.1080/08850607.2013.807188

Hicks, D. (2016). *The construction of librarians' professional identities: a discourse analysis.* (Unpublished doctoral thesis). University of Alberta, Edmonton, Canada. https://doi.org/10.7939/R3VQ2SJ66

Hunter, L. (2012). Challenging the reported disadvantages of e-questionnaires and addressing methodological issues of online data collection. *Nurse Researcher, 20*(1), 11-20. https://doi.org/10.7748/nr2012.09.20.1.11.c9303

Ibarra, H. (1999). Provisional selves: experimenting with image and identity in professional adaptation. *Administrative Science Quarterly, 44*(4), 764-791. https://doi.org/10.2307/2667055

Idowu, B. (2017). Counselling psychologists' experience of their professional identity whilst working in an IAPT service: an interpretative phenomenological analysis (Unpublished doctoral thesis). London Metropolitan University, London, UK. Retrieved from https://core.ac.uk/download/pdf/84654165.pdf

Jacob, S., & Boisvert, Y. (2010). To be or not to be a profession: pros, cons and challenges for evaluation. *Evaluation 16*(4), 349–369. https://doi.org/10.1177/1356389010380001

Jebril, M. Y. A. (2008). *The evolution and measurement of professional identity.* (Unpublished doctoral dissertation). Texas Woman's University, Denton, US. Retrieved from https://twu-ir.tdl.org/handle/11274/10773

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research, 1*(2), 112-133. https://doi.org/10.1177/1558689806298224

Johnsson, L., Eriksson, S., Helgesson, G., & Hansson, M. G. (2014). Making researchers moral: Why trustworthiness requires more than ethics guidelines and review. *Research Ethics, 10*(1), 29-46. https://doi.org/10.1177/1747016113504778

Johnston, R. (2005). *Analytic culture in the US intelligence community: An ethnographic study*. Washington, D.C: Center for the Study of Intelligence, Central Intelligence Agency. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/analytic_culture_report.pdf

Kerbel, J. (2008). Lost for words: The intelligence community's struggle to find its voice. *Parameters*, *38*(2), 102-112. Retrieved from https://press.armywarcollege.edu/parameters/vol38/iss2/13

Kreiner, G. E., & Ashforth, B. E. (2004). Evidence toward an expanded model of organizational identification. *Journal of Organizational Behavior, 25*(1), 1-27. https://doi.org/10.1002/job.234

Kreiner, G. E., Hollensbe, E. C., & Sheep, M. L. (2006). Where is the "me" among the "we"? Identity work and the search for optimal balance. *Academy of Management Journal, 49*(5), 1031-1057. Retrieved from https://www.jstor.org/stable/20159815

Kumpusalo, E., Neittaanmäki, L., Mattila, K., Virjo, I., Isokoski, M., Kujala, S., Luhtala, R. and Jääskeläinen, M. (1994). Professional identities of young physicians: A Finnish national survey. *Medical Anthropology Quarterly*, *8*(1), 69-77. https://doi.org/10.1525/maq.1994.8.1.02a00050

Larkin, M., Watts, S., & Clifton, E. (2006). Giving voice and making sense in interpretative phenomenological analysis. *Qualitative Research in Psychology, 3*(2), 102-120. https://doi.org/10.1191/1478088706qp062oa

Lavrakas, P. (2008). *Encyclopedia of survey research methods.* Thousand Oaks, California. https://doi.org/10.4135/9781412963947

Leech, N. L., & Onwuegbuzie, A. J. (2009). A typology of mixed methods research designs. *Quality and Quantity, 43*(2), 265-275. https://doi.org/10.1007/s11135-007-9105-3

Levin-Rozalis, M., & Shochot-Reich, E. (2009). Professional identity of evaluators in Israel. *The Canadian Journal of Program Evaluation, 23*(1), 141-177. Retrieved from https://www.academia.edu/11679934/Professional_Identity_of_Evaluators_in_Israel

Li, M., & Chitty, N. (2017). Paradox of professionalism: The professional identity of journalists who work across media cultures. *Journalism*. https://doi.org/10.1177/1464884917743175

Liu, Y., Lam, L. W., & Loi, R. (2014). Examining professionals' identification in the workplace: The roles of organizational prestige, work-unit prestige, and professional status. *Asia Pacific Journal of Management*. *31*(3). 789-81. https://doi.org/10.1007/s10490-013-9364-6

Mael, F., & Ashforth, B. E. (1992). Alumni and their alma mater: A partial test of the reformulated model of organizational identification. *Journal of Organizational Behavior, 13*(13), 103-123. https://doi.org/10.1002/job.4030130202

Manojlovic, D. (2014). Intelligence analysis in corporate security. *Megatrend Review, 11*(4), 301-320. Retrieved from https://www.researchgate.net/publication/277887752_Intelligence_analysis_in_corporate_security

Marks, D. F., & Yardley, L. (2004). Content and thematic analysis. In *Research Methods for Clinical and Health Psychology*, 56-68. https://dx.doi.org/10.4135/9781849209793.n4

Mellin, E. A., Hunt, B., & Nichols, L. M. (2011). Counselor professional identity: findings and implications for counselling and interprofessional collaboration. *Journal of Counseling and Development, 89*(2), 140-148. https://doi.org/10.1002/j.1556-6678.2011.tb00071.x

Mercurio, Z. A. (2019). *The lived experience of meaningful work in a stigmatized occupation: A descriptive phenomenological inquiry*. (Doctoral dissertation) Colorado State University, Fort Collins, Colorado, US. Retrieved from https://hdl.handle.net/10217/197411

Messenger, K., Farquharson, L., Stallworthy, P., Cawkill, P., & Greenberg, N. (2012). The experiences of security industry contractors working in Iraq: An interpretative phenomenological analysis. *Journal of Occupational and Environmental Medicine*, *54*(7), 859-867. https://doi.org/10.1097/JOM.0b013e31824e676b

Miscenko, D., & Day, D. V. (2016). Identity and identification at work. *Organizational Psychology Review*, *6*(3), 215-247. https://doi.org/10.1177/2041386615584009

Molleman, E., & Rink, F. (2013). Professional identity formation amongst medical specialists. *Medical Teacher*, *35*(10), 875-876. Retrieved from https://www.researchgate.net/profile/Eric_Molleman/publication/256835695_Professional_Identity_Formation_amongst_Medical_Specialists/links/0c9605281dff477263000000.pdf

Molleman, E., & Rink, F. (2015). The antecedents and consequences of a strong professional identity among medical specialists. *Social Theory & Health*, *13*(1), 46-61. https://doi.org/10.1057/sth.2014.16

Moore, D. T., Krizan, L., & Moore, E. J. (2005). Evaluating intelligence: A competency-based model. *International Journal of Intelligence and CounterIntelligence*, *18*(2), 204-220. https://doi.org/10.1080/08850600590911945

Morgan, D. L. (2014). Pragmatism as a paradigm for mixed methods research. In *Integrating qualitative and quantitative methods: a pragmatic approach*, 25-44. SAGE Publications Ltd. https://doi.org/10.4135/9781544304533

N Pam, M. (2013). *Valence*. Retrieved from https://dictionary.apa.org/valence

Neary, S. (2014). Professional Identity: What I call myself defines who I am. *Career Matters, 2*(3), 14-15. Retrieved from https://core.ac.uk/download/pdf/46170813.pdf

Nikendei, C., Ben-David, M. F., Mennin, S., & Huwendiek, S. (2016). Medical educators: How they define themselves: Results of an international web survey. *Medical Teacher, 38*(7), 715-723. https://doi.org/10.3109/0142159X.2015.1073236

Nuttman-Shwartz, O. (2017). Rethinking professional identity in a globalized world. *Clinical Social Work Journal, 45*(1), 1-9. https://doi.org/10.1007/s10615-016-0588-z

Office for National Statistics. (2019). *UK SIC 2007*. Retrieved from https://www.ons.gov.uk/methodology/classificationsandstandards/ukstandardindustrialclassificationofeconomicactivities/uksic2007

O'Flaherty, M., Ulrich, G. (2016). The professional identity of the human rights field officer. Routledge.

Pallant, J. (2003). SPSS survival manual: a step by step guide to data analysis using SPSS. Routledge.

Pate-Cornell, E. (2015). Uncertainties, intelligence, and risk management: a few observations and recommendations on measuring and managing risk. *Stanford Journal of International Law, 51*(1), 53-67. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.stanit51.7&site=eds-live

Petersen, K. L. (2013). The corporate security professional: A hybrid agent between corporate and national security. *Security Journal, 26*, 222-235. https://doi.org/10.1057/sj.2013.13

Petersen, K. L., & Tjalve, V. S. (2018). Intelligence expertise in the age of information sharing: public-private 'collection' and its challenges to democratic control and accountability. *Intelligence and National Security, 33*(1), 1-15. https://doi.org/10.1080/02684527.2017.1316956

Pietkiewicz, I., & Smith, J. A. (2014). A practical guide to using Interpretative Phenomenological Analysis in qualitative research psychology. *Psychological Journal*, *20*(1), 7-14. Retrieved from

https://www.researchgate.net/publication/263767248_A_practical_guide_to_using_Interpretative_Phenomenological_Analysis_in_qualitative_research_psychology

Plett, M., Hawkinson, C., Vanantwerp, J. J., Wilson, D., & Bruxvoort, C. (2011). Engineering identity and the workplace persistence of women with engineering degrees. In *American Society for Engineering Education*. American Society for Engineering Education. Retrieved from https://www.researchgate.net/publication/257633106_Engineering_Identity_and_the_Workplace_Persistence_of_Women_with_Engineering_Degrees

Pratt, M. G., Rockmann, K. W., & Kaufmann, J. B. (2006). Constructing professional identity: The role of work and identity learning cycles in the customization of identity among medical residents. *Academy of Management Journal, 49*(2), 235-262. https://doi.org/10.5465/AMJ.2006.20786060

Randolph, J. (2009). A guide to writing the dissertation literature review. *Practical Assessment, Research and Evaluation, 14*(13). https://doi.org/10.7275/b0az-8t74

Reed, M. I. (1996). Expert power and control in late modernity: an empirical review and theoretical synthesis. *Organization Studies, 17*(4), 573-597. https://doi.org/10.1177/017084069601700402

Rehn, A. (2012). Indier than thou: On creative professions, chefs, and the sacralization of margins. *ephemera, 12*(3), 344-354. Retrieved from http://www.academia.edu/download/27903872/12-3ephemera-aug12.pdf#page=88

Rewolinski, C. (2014). *The measurement of occupational identity among undergraduate preservice music teachers: a test development study.* (Doctoral dissertation), University of North Texas, Denton, Texas. Retrieved from https://digital.library.unt.edu/ark:/67531/metadc699995/

Roberts, L. M., & Creary, S. J. (2013). Navigating the self in diverse work contexts. In Q. Roberson (Ed.), *The Oxford handbook of diversity and work,* 73-97. New York: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199736355.013.0005

Robson, C., & McCartan, K. (2016). *Real-world research* (4th edition). Chichester, UK: John Wiley & Sons.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students*. (5th edition) Pearson education.

Shaeffer, M. K. (2016). *Professional identity and professionalization in archaeology: a sociological view*. Kent State University, Ohio, US. Retrieved from http://rave.ohiolink.edu/etdc/view?acc_num=kent1476888346964438

Schaub, Jr, G., & Franke, V. (2009). Contractors as military professionals? *Parameters*, US Army War College, *39*(4), 88-104. Retrieved from https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1024&context=facpubs

Shinebourne, P. (2011). The theoretical underpinnings of interpretative phenomenological analysis (IPA). *Existential Analysis: Journal of the Society for Existential Analysis, 22*(1), 16-32.

Smith, J. A., Flowers, P., & Larkin, M. (2009). *Interpretative Phenomenological Analysis: Theory, method and research*. London: SAGE Publications Ltd.

Smith, S. (2016). *An exploration of professional identity in the information technology sector.* (Doctoral dissertation), Edinburgh Napier University. UK. Retrieved from https://www.napier.ac.uk/~/media/worktribe/output-169780/an-exploration-of-professional-identity-in-the-information-technology-sector.docx

Spracher, W. C. (2009). *National security intelligence professional education: a map of US civilian university programs and competencies*. (Doctoral dissertation), The George Washington University, Washington, DC, US. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.604.7161&rep=rep1&type=pdf

Stets, J. E., & Burke, P. J. (2003). A sociological approach to self and identity. In M. Leary & J. Tangney (Eds.), *Handbook of self and identity*, 128-152. New York: Guilford

Publications. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.540.6343&rep=rep1&type=pdf

Stets, J. E., & Burke, P. J. (2000). Identity theory and social identity theory. *Social Psychology Quarterly, 63*(3), 224-237. https://doi.org/10.2307/2695870

Stryker, S., & Burke, P. J. (2000). The past, present, and future of an identity theory. *Social Psychology Quarterly, 63*(4), 284-297. https://doi.org/10.2307/2695840

Sullivan, K. (2012). Producing professionals: Exploring gendered and embodied responses to practicing on the margins. *Ephemera, 12*(3), 273-293. Retrieved from http://www.academia.edu/download/27903872/12-3ephemera-aug12.pdf#page=17

Sylvia, C. J. (2018). Exploring the identity of the certified wound ostomy continence nurse in industry: An interpretive analysis of professional ecology. (Doctoral dissertation), Cardiff University, UK. Retrieved from http://orca.cf.ac.uk/id/eprint/113359

Tajfel, H. (1982). Social psychology of intergroup relations. *Annual Review of Psychology, 33*(1), 1-39. Retrieved from https://pdfs.semanticscholar.org/45a2/334a518e1e0069079ce25e81aa5c637415fe.pdf

Tajfel, H., Billig, M. G., Bundy, R. P., & Flament, C. (1971). Social categorization and intergroup behaviour. *European Journal of Social Psychology*, *1*(2), 149-178. https://doi.org/10.1002/ejsp.2420010202

Tajfel, H., & Turner, J. C. (2004). The social identity theory of intergroup behavior. In J. T. Jost & J. Sidanius (Eds.), *Political Psychology: Key Readings*, 276-293. New York: Psychology Press. Retrieved from http://christosaioannou.com/Tajfel%20and%20Turner%201986.pdf

Tashakkori, A., & Teddlie, C. B. (1998). *Mixed methodology: Combining qualitative and quantitative approaches.* Applied social research methods series, Vol. 46. Sage Publications.

Thomas, C. L. (2016). *The role of occupational branding in the professionalization of technical communication.* (Masters thesis), University of Central Florida, Orlando, US. Retrieved from http://etd.fcla.edu/CF/CFE0006189/Thomas_Thesis.pdf

Thornhill, A., Saunders, M., & Lewis, P. (2009). *Research methods for business students.* Essex: Pearson Education Ltd. Retrieved from https://www.researchgate.net/publication/309102603_Understanding_research_philosophies_and_approaches

Tomkins, L., & Eatough, V. (2018). Hermeneutics: Interpretation, Understanding and Sense-making. In Cassell, Catherine; Cunliffe, Ann L. and Grandy, Gina (eds.) *The SAGE Handbook of Qualitative Business and Management Research Methods: History and Traditions*. 185-200. Sage Publications. https://dx.doi.org/10.4135/9781526430212

Topp, K. D. (2015). *Managing different roles: The experiences of female nursing reservists who have deployed with the UK armed forces.* (Doctoral dissertation), University of Hull, Kingston-upon-Hull, UK. Retrieved from https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.684221

Tsakissiris, J. (2015). *The role of professional identity self-interest in career choices in the emerging ICT workforce* (Masters thesis), Queensland University of Technology, Brisbane, Australia). Retrieved from https://eprints.qut.edu.au/91646/1/Jane_Tsakissiris_Thesis.pdf

Tuffour, I. (2017). A critical overview of Interpretative Phenomenological Analysis: A contemporary qualitative research approach. *Journal of Healthcare Communications, 2*(4), 52. https://doi.org/10.4172/2472-1654.100093

Turner, J. C., & Reynolds, K. J. (2012). Self-categorization theory. In P. A. Van Lange, A. W. Kruglanski, & E. T. Higgins (Eds.), *Handbook of Theories of Social Psychology* (2nd ed.) pp. 399-417. London: SAGE Publications Ltd. http://dx.doi.org/10.4135/9781446249222.n46

UNESCO Institute for Statistics. (2015). I*nternational Standard Classification of Education: 2013 Fields of Education and Training (ISCED-F 2013) Descriptions*. Retrieved from UNESCO Digital Library website: https://unesdoc.unesco.org/ark:/48223/pf0000235049

Verling, R. (2014). *Exploring the professional identity of counselling psychologists: a mixed methods study*. (Doctoral thesis), University of Wolverhampton, UK. Retrieved from https://wlv.openrepository.com/handle/2436/335796

Voelz, G. J. (2009). Contractors and intelligence: The private sector in the intelligence community. *International Journal of Intelligence and CounterIntelligence, 22*(4), 586-613. https://doi.org/10.1080/08850600903143106

Warren, A. F. (2014). *Innovation, personal growth and professional identity: perspectives on role emerging placements in occupational therapy*. (Doctoral thesis), University of Limerick, Ireland. Retrieved from https://ulir.ul.ie/handle/10344/3996

Weiss-Gal, I., & Welbourne, P. (2008). The professionalisation of social work: A cross-national exploration. *International Journal of Social Welfare, 17*(4), 281-290. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1468-2397.2008.00574.x

Wilkinson, A., Hislop, D., & Coupland, C. (2016). The changing world of professions and professional workers. In *Perspectives on Contemporary Professional Work: Challenges and Experiences,* 3-15. https://doi.org/10.4337/9781783475582.00009

Willig, C. (2013). Introducing qualitative research in psychology. McGaw-Hill Education.

Woo, H., Lu, J., & Bang, N. (2018). Professional Identity Scale in Counseling (PISC): Revision of factor structure and psychometrics. *Journal of Counselor Leadership and Advocacy. 5*(2), 137-152. Retrieved from https://www.tandfonline.com/doi/full/10.1080/2326716X.2018.1452078

Wood, C., Goodall, D., & Farmer, M. D. (2016). Changing professional identity in the transition from practitioner to lecturer in Higher Education: An Interpretive

Phenomenological Analysis. *Research in Post-Compulsory Education*, *21*(3), 229-245. https://doi.org/10.1080/13596748.2016.1195173

Zimmermann, D. (2011). The Security Intelligent Enterprise. *International Journal of Intelligence and CounterIntelligence*, 24(3), 569–574. https://doi.org/10.1080/08850607.2011.548216

Appendices

APPENDIX A

Literature search strategy used in the study

Parameter	Narrow	Broad (Key words/search terms/approach)
Language	English (US & UK)	Other language that I could understand (Dutch) or articles that were translated from the original to English.
Focus	Research methods & findings, theories practices or applications	Extent of empirical research, key variables, measurement, methods of analysis, strength and weaknesses of existing literature, relationship between theories, phenomenon, gaps
Subject Area	Security risk analysis	Security management, privatisation of security/intelligence, outsourcing, contractors, embedded analysts.
	Intelligence analysis	Intelligence, analytical tradecraft, threat analysis, security intelligence, protective intelligence, security/intelligence expertise, skills set, values & ethics, management of intelligence, attributes
	Professional identity	Occupational/work/career/vocational identity OR image OR perception OR commitment OR perspectives, organisational identity, identity construction, corporate culture, identity management, ethics, values, identity conflicts, professional agency, professional perceptions, professional reinvention, socio-cultural elements
	Professions, professionalism & professionalisation	Organisational Studies, Sociology of professions, emerging professions, globalisation, the new world of work, knowledge-intensive firms, knowledge workers, hybrid professionalism, professional development, power relations
	Identity theories	Social theory, self-categorisation, self-identification, individual identity, collective identity, group identity, organisational identity, psychology, sociology, social psychology
Business area	Private/Corporate security risk OR intelligence	Private/Corporate security, general consulting firms, cross-domain international companies, intelligence and risk consulting
Geographical area	International	Global, multinational, transnational
Publication period	Last 10 years	Last 30 years
Literature type	Refereed journals, conference proceedings and academic books	Professional magazines, journals, websites of companies and professional organisations

APPENDIX B

Typical job advertisements for security risk intelligence analysts in the private sector

Intelligence Analyst I - Regional

WorldAware Solutions (PTY) LTD, Block A, The Terraces, Cape Town, South Africa, South Africa
Req #246
Date Posted: Thursday, December 5, 2019

At WorldAware, we take a proactive approach to solving business challenges and our customers are at the heart of everything we do. It's the reason we love rolling up our sleeves and getting down to work – and it's why we're so successful. It takes an entire team to stand behind something big. Interested?

Position Overview:

Join the WorldAware Risk Intelligence Team! Be part of our global Africa team. We will rely on you to be the intelligence Sherpa for our clients, specifically in the Southern African Region. Do what you love, monitor real-time events in Africa, prioritize those situations of concern to our clients, and hone your writing and analytical skills as part of a best in class intelligence organization. You will draft well-written intelligence products with minimal supervision. You will deliver timely, accurate, and relevant intelligence in the form of brief tactical alerts, situation reports, in-depth assessments, and strategic predictions. In addition, you will be challenged to respond professionally to quick-turnaround client requests in writing and/or on the telephone and may be called upon to conduct client-facing webinars. We are Looking for a self-starter, someone who is calm under pressure, and has demonstrated high-quality writing and briefing skills.

Shift work and flexibility in scheduling is required to meet our 24/7/365 mission.

Essential Duties/Responsibilities:

- Be the subject matter expert for Africa (Southern Africa)
- Monitors events and developments in region for alerting and general awareness
- Drafts concise, accurate, error-free intelligence
- Peer support for other Africa sub-regions and global regions
- Interacts professionally with clients in written and verbal communications

Experience, Functional and Technical Requirements:

- Bachelor's degree in a related discipline required (Political Science, Economics, International Relations, Intelligence); Master's preferred
- 2+ years' experience in a related field preferred (Intelligence, Analysis, Security, Risk Management)
- Foreign language proficiency preferred
- Regional work/study experience

Skills/Abilities:

- Excellent intelligence gathering and analytic skills
- Excellent written and verbal skills
- Excellent computer skills
- Management and leadership skills
- Inter-personal skills
- Effective time management and problem solving skills
- Ability to organize and prioritize work with little supervision

An international security risk/intelligence consultancy with offices in US, UK, South Africa

Global Security Analyst

As a member of Stratfor's core team of analysts, you will be responsible for developing high-quality and forward-looking analysis related to corporate security, business continuity, cyber security, organized crime, and global terrorism. Analysts are responsible for ensuring that a broad range of clients are well served by proactively identifying critical crime, terrorism and business continuity issues while conducting deeper research on key topics to include terror and criminal attack cycles, and cyber-attack tactics. Stratfor Threat Lens helps corporate security leaders identify, anticipate, measure and mitigate risks that emerging threats pose to their people, assets and interests around the world. Clients rely on Threat Lens to pinpoint which evolving global events are truly significant so they can save time and make decisions with confidence.

Analysts also play a critical role in the Stratfor forecasting process and production of the Geopolitical Risk Index and Geopolitical Risk Monitor. Analysts have direct engagement with clients supporting inbound geopolitical inquiries while providing briefings.

Global Security Analysts will have the opportunity to partner with colleagues across the broader RANE organization and gain exposure to a ra industries and risk topics, including geopolitical; cyber and information; physical safety and security; and legal, regulatory, and compliance.

Responsibilities

- Conducting research and analysis leveraging open source, as well as proprietary content/ data sets, and in-house subject matter expert
- Daily production of analytic content for distribution to Threat Lens client base
- Regular contributions to longer-form analytic pieces
- Active participation in quarterly, annual, and 10-year forecasting process
- Conducting RANE Expert interviews on key topical issues, as an input to content pieces or client inquiries
- Participating in calls to support current and potential Threat Lens clients.

Key Skills and Competencies

- Creativity and clarity in constructing clear, logical arguments with supporting evidence; Strong analytical and critical thinking skills
- Excellent writing, research, briefing, and editorial capabilities—strong command of English grammar
- Rigor and resourcefulness in conducting research
- Well-rounded and in-depth understanding of global terrorism, cyber security, and personnel threat issues to include travel security and workplace threat issues
- Ability to multi-task and work on multiple, time-sensitive client projects in a fast-paced, deadline-driven professional environment
- Ability to work collaboratively and effectively across multiple internal teams and stakeholders; flexibility and ability to adapt quickly to changing requirements is critical
- Entrepreneurial and proactive approach to work; ability to independently synthesize information and resources to identify opportunities and solutions

Qualifications

- Master's Degree preferred
- Bachelor's Degree with demonstrated academic achievement required
- 2-4+ years relevant work experience
- Exceptional oral and written communication skills
- Previous qualitative research and report-writing experience in a professional domain required
- Demonstrated sense of initiative and curiosity, willingness to ask questions and get answers
- Ability to meet deadlines and multi-task in a fast-paced environment
- Ability to function in a start-up atmosphere, comfort with ambiguity and change

Additional Requirements

- Role will be based in Austin, TX
- Candidates will be required to provide a writing sample

A US based think tank/network organisation

https://ranenetwork.com/careers/#1583861496468-70abbfa1-e976

APPENDIX C1

Survey

Who are we? The professional identity of security risk intelligence analysts in the private sector: an international perspective

Page 1: Introduction

The professional identity of security risk intelligence analysts in the private sector

We would like to invite you to take part in our research study. Before you decide, we would like you to understand why the research is being conducted and what it would involve for you.

The questionnaire has been produced in part completion of a Prof Doc in Security Risk Management at the University of Portsmouth, U.K.

What is the purpose of the study?

The purpose of this study is to collect information about how Security Risk Intelligence Analysis practitioners, across different organisational contexts and national boundaries, construct their individual and collective professional identity in their quest to make a meaningful contribution to society.

Why have I been invited?

focus on managing and/or conducting the analysis and interpretation of the possible impact of external and internal threats on the company or your client. You should be working in the private or NGO sectors, and no government or law enforcement analysts are included in this survey. Your job title would be any of the following: security risk or threat analyst, crime analyst, crime intelligence analyst, research specialist, political risk analyst, cyber threat analyst, intelligence manager, security risk manager etc. You should be doing any or all of the following:

- Monitoring geo-political and socio-economic developments in countries where their company/clients have interests, including conducting travel risk analysis services to personnel;
- Analysing and advising on the prevention of cyberattacks against the company/client from the wide array of threat actors;
- Advising on criminal activities that might impact the company's physical and personnel protection operations, as well as its service and product delivery;
- Monitoring reputational and other socio-political risks against the company;
- Conducting due diligence investigations to ensure the resilience of the company's supply and delivery chains;
- Investigating personnel integrity risks and/or
- Conducting strategic analysis and advising on the company's strategic security management.

Do I have to take part?

There is no obligation to take part and it is entirely up to you to decide whether you would like to join the study.

What will happen to me if I take part?

All responses are entirely confidential and anonymous. All data collected will be held securely and password protected. The survey will take you around **20** minutes to complete.

Expenses and payments

The survey is free to complete and there is no cost to you apart from your time. No expense, payments or incentives are available.

What will I have to do?

If you agree to take part, you will be asked to complete a set of online survey questions.

What are the possible disadvantages and risks of taking part?

The online survey will take around **20** minutes to complete. Aside from using your time, no disadvantages are anticipated. Your identity will never be revealed in the dissertation or any published material, and all data will be presented in aggregated and summary format.

What are the possible benefits of taking part?

Whilst it is unlikely that you will receive any direct benefit as a result of taking part in the study, you will be contributing towards important academic research. Such enhancements could be of benefit to you, your colleagues and the individuals you interview in your line of work.

Will my taking part in the study be kept confidential?

Yes. All responses are entirely confidential. All reasonable steps to retain anonymity will be maintained. The survey will not ask you to reveal any personal identifying information. Your data will be collected online through the online survey tool JISC Online Survey. The survey can only be accessed by the lead researcher Dalene Duvenage and will be password protected.

Current data retention guidelines for researchers at the University of Portsmouth have to comply with mean that the aggregated datasets will be securely stored for at least 10 years.

What will happen if I don't want to carry on with the study?

All questions are optional. If you wish to abandon the survey before completion, you can simply leave the website or simply miss out any questions you would rather not answer.

If you complete all or part of the survey, but then decide you would like to with draw your data, please be aware that this may not be possible due to the anonymous nature of online surveys.

What if there is a problem?

If you have a concern about any aspect of this study, you should ask to speak to the researcher or their supervisor, who will do their best to answer your questions. The researcher, Dalene Duvenage, can be contacted at magdalena.duvenage@myport.ac.uk or supervisor/gatekeeper, Dr Moufida Sadok, can be contacted at moufida.sadok@port.ac.uk . If you remain unhappy and wish to complain formally, you can do this by contacting the head of school, at Paul.Norman@port.ac.uk or the ICJS Ethics Committee chair on vasileios.karagiannopoulos@port.ac.uk.

What will happen to the results of the research study?

The results may form part of the researcher's dissertation and it may also form part of a published paper or book at a later date. Aggregated findings may also be presented at relevant conferences. You will not be personally identified in any publication.

Who is organising and funding the research?

By continuing with the survey you agree that:

1. You have read and understand the Information presented for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.
2. You understand that your participation is voluntary and that you are free to withdraw at any time without giving any reason.
3. You understand that data collected during the study, may be looked at by research staff from

Page 2: Demographics

1. What is your age?

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65+

2. What is your gender?

3. How many total years' experience do you have in the security risk intelligence analysis field?

- 1-5 years
- 6-10 years
- 11-15 years
- 16-20 years
- 21-25 years
- More than 25 years

4. Have you previously worked for government/law enforcement and then moved to the private sector?

5. What is your country of citizenship?

5.a. In which country do you work, if you are NOT working in your own country? *Optional*

6. What is your official job title?

6.a. What other job title would fit what you are doing? *Optional*

7. Are you currently in a supervisory/management role?

- Yes
- No

8. In what sector are you currently working? (Choose ONE from the list of UK Standard Industrial Classification - SIC) https://uksiccodes.com/siccodesuk.html

8.a. If you selected Other, please specify:

9. What is the type of organisation/company you currently work for?

- Self-employed
- A private security company with its own security risk intelligence analysis capacity.
- A security/intelligence/risk unit in a private company/multinational corporation whose core business is not security.
- A private local/national/multinational company who provide security risk intelligence consulting services to external clients, including the private sector or government agencies. This would therefor also include contractors working in situ at government departments/agencies.
- A non-governmental organisation (NGO) with its own security risk intelligence analysis capacity.
- An intergovernmental organisation (IGO) with its own security risk intelligence analysis capacity.
- Research institute/foundations/think tanks whose primary function is to provide security risk intelligence analysis and advice to external clients.
- Independent regulatory/supervisory body..
- Do not want to disclose
- Other

9.a. If you selected Other, please specify:

10. What are the focus area/s of your analytical reports or advice that you provide to your clients?

- [ ] Cyber threat analysis
- [ ] Analytical practices
- [ ] Corruption
- [ ] Cyber threats
- [ ] Environmental crime/risks
- [ ] Espionage threats
- [ ] Executive protection
- [ ] Extremism
- [ ] Fixated/psychological disturbed persons of interest
- [ ] General crime
- [ ] Geo-political developments
- [ ] Governance and/or compliance
- [ ] Insider threats
- [ ] Interest and pressure groups of interest to the client
- [ ] Internal investigations
- [ ] Loss prevention
- [ ] Military threats
- [ ] Money laundering and fraud
- [ ] National political developments
- [ ] Organised crime
- [ ] Personnel security incidents
- [ ] Physical protection of facilities
- [ ] Political economy developments
- [ ] Reputational risks
- [ ] Security management strategy
- [ ] Security risk management
- [ ] Socio-economic developments
- [ ] Strategic analysis & Foresight
- [ ] Strategic security management
- [ ] Terrorism & counter-terrorism
- [ ] Terrorist financing
- [ ] Travel risk
- [ ] Other

11. What is your highest completed qualification? (Choose ONE)

- ○ High School/secondary school
- ○ 1 or 2 year qualification
- ○ Bachelors degree (3/4 years) or equivalent
- ○ Honours degree (1yr after Bachelors) or equivalent
- ○ Masters degree
- ○ Doctorate degree
- ○ Post-doc degree
- ○ Do not want to disclose

12. In which field did you obtain your highest qualification? (Choose ONE from Unesco ISCED-F list)

- ○ Education
- ○ Arts and humanities including languages
- ○ Social sciences, journalism and information including Economics, political sciences, psychology, sociology
- ○ Business, administration and law including accounting, management, finance etc
- ○ Natural sciences, mathematics and statistics
- ○ Information and Communication Technologies (ICTs)
- ○ Engineering, manufacturing and construction
- ○ Agriculture, forestry, fisheries and veterinary
- ○ Health and welfare
- ○ Services including security, military, law enforcement
- ○ Do not want to disclose

13. Do you belong to a professional organisation? ✱ *Required*

- ○ Yes
- ○ No

13.a. Which professional organisation/s? (list with commas in between)

13.a.i. Why are you a member of professional organisation/s?

13.b. Why are you **NOT** a member of a professional organisation/s?

Page 3: Role and function

14. **In your experience what is the main role and function of Security Risk Intelligence Analysts in the private sector?**

15. **In your experience what is the unique contribution of Security Risk Intelligence Analysts to the private sector and to society?**

Page 4: How do you define your professional identity?

16. Please rate the extent to which you agree with each of the following statements:

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
Generally, the more my goals, values, and beliefs overlap with those of my profession, the happier I am.	☐	☐	☐	☐	☐
I would rather say 'we' than 'they' when talking about the profession I work in.	☐	☐	☐	☐	☐
I strongly define myself as a Security Risk Intelligence Analysis professional.	☐	☐	☐	☐	☐
I'm not interested in what others think about the Security Risk Intelligence Analysis profession.	☐	☐	☐	☐	☐
I currently attend /would like to attend events where Security Risk Intelligence Analysis best practice are shared.	☐	☐	☐	☐	☐
When someone praises the Security Risk Intelligence Analysis profession, it feels like a personal compliment.	☐	☐	☐	☐	☐

If a story in the media criticized the Security Risk Intelligence Analysis profession, I would feel embarrassed e.g. the case of Reality Winner, a US intelligence analysis contractor who was sentenced to jail in June 2018 after she leaked information to the media.	☐	☐	☐	☐	☐
All other factors being equal, I would rather change my employer than my profession as a Security Risk Intelligence Analyst.	☐	☐	☐	☐	☐
It is more important that I conduct my work professionally, than being a member of a specific "profession".	☐	☐	☐	☐	☐

17. Please rate the extent to which you agree with each of the following statements:

Please don't select more than 1 answer(s) per row.

Please select at least 5 answer(s).

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
I think highly of the Security Risk Intelligence Analysis profession.	☐	☐	☐	☐	☐
I consider it prestigious to belong to the Security Risk Intelligence Analysis profession.	☐	☐	☐	☐	☐
I consider the Security Risk Intelligence Analysis profession to be one of the best professions for people with the relevant skills and education.	☐	☐	☐	☐	☐
I would not recommend this career to someone else.	☐	☐	☐	☐	☐
I see a future for myself being a Security Risk Intelligence Analysis in the private sector and would like to remain in this profession in some capacity.	☐	☐	☐	☐	☐

Page 5: Opportunities and challenges

18. **What benefits/opportunities do you derive from being a Security Risk Intelligence Analyst? Name at least 2.**

19. **In your experience, what are the 3 biggest challenges you experience/d as a Security Risk Intelligence Analyst?**

Page 6: Perception by others

20. Please rate the extent to which you agree with each of the following statements:

Please don't select more than 1 answer(s) per row.

Please select at least 5 answer(s).

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
People in general think highly of the Security Risk Intelligence Analysis profession.	☐	☐	☐	☐	☐
It is considered prestigious to belong to the Security Risk Intelligence Analysis profession.	☐	☐	☐	☐	☐
The Security Risk Intelligence Analysis profession is considered to be one of the best professions.	☐	☐	☐	☐	☐
Most of the stakeholders with whom I liaise, value the contribution I, as a Security Risk Intelligence Analyst, make to achieve our mandate.	☐	☐	☐	☐	☐
My management and/or clients do not have good perception of the profession of the Security Risk Intelligence Analysis.	☐	☐	☐	☐	☐

Page 7: Professionalism

21. In your experience, what are the 3 most important/ non-negotiable professional values/ethical standards or codes of conduct that you practise as a Security Risk Intelligence Analyst?

22. What is your definition of a "professional"?

23. In your opinion, what would help to strengthen the identity of the Security Risk Intelligence Analysis profession?

24. In light of the fast changing working environment, what skills do you think security risk intelligence analysts need to acquire to stay relevant in the future? *Optional*

Page 8: Thank you! Do you want to participate in the interviews?

If you would like to participate in the follow-up interviews, please contact me at Magdalena.Duvenage@myport.ac.uk

Thank you for your participation!

Key for selection options

4 - Have you previously worked for government/law enforcement and then moved to the private sector?

- Yes
- No

8 - In what sector are you currently working? (Choose ONE from the list of UK Standard Industrial Classification - SIC) https://uksiccodes.com/siccodesuk.html

- Agriculture
- Mining & Quarrying
- Manufacturing
- Electricity, Gas, Steam and Air Conditioning
- Water Supply, Sewerage, Waste Management
- Construction
- Wholesale and Retail trade; repair of vehicles
- Transport & Storage
- Accommodation and Food service
- Information & Communication
- Finance & Insurance
- Real Estate
- Professional, Scientific & Technical
- Admin & support service activities
- Public Sector, Social Security & Defence
- Education
- Human Health & Social Work
- Arts, Entertainment & Recreation
- Other service activities
- Household employers & Goods for own use
- Extraterritorial Organisations & Bodies
- Do not want to disclose

APPENDIX C2

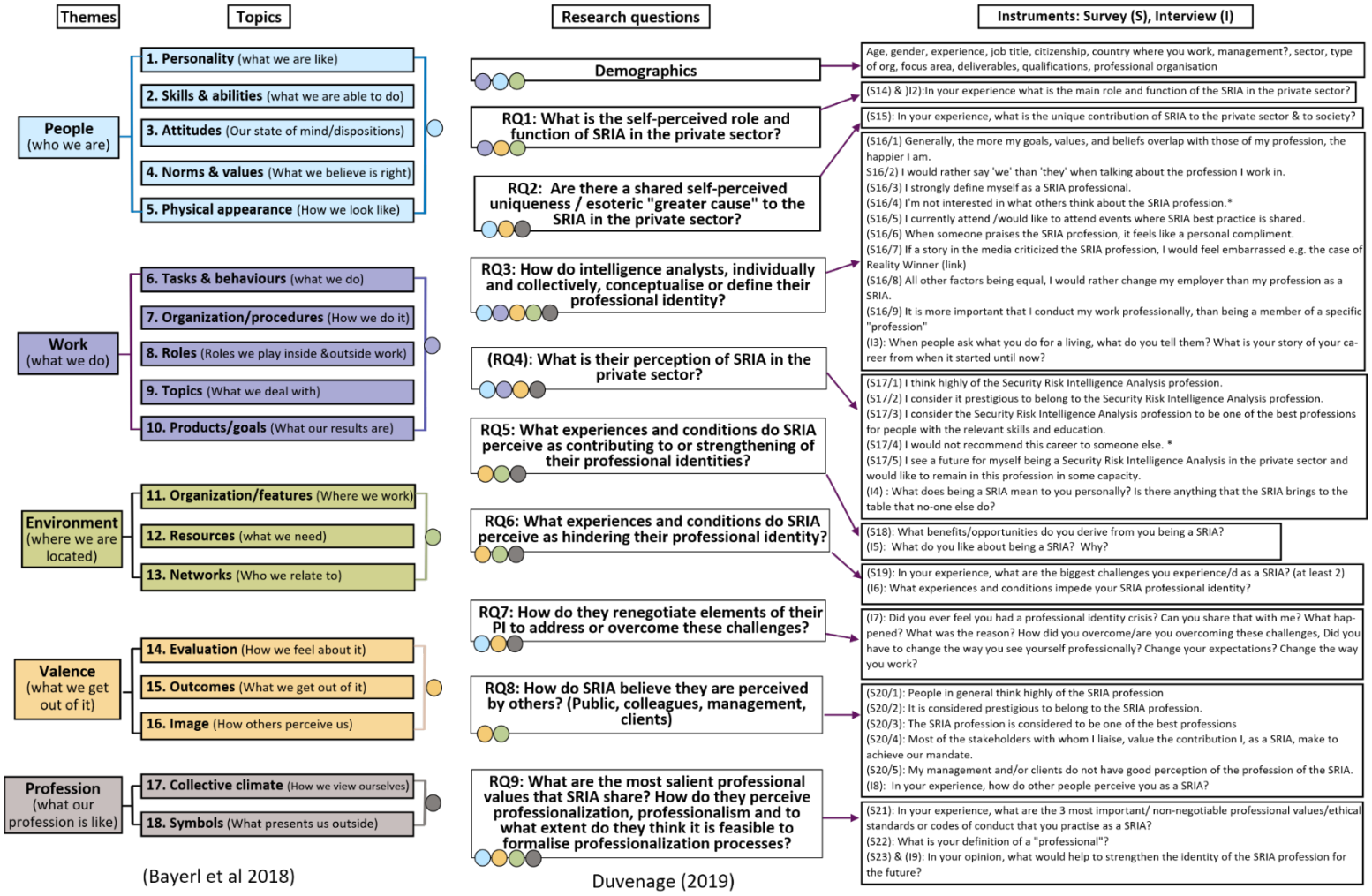
Research questions and the related survey questions

	Research questions	Survey Questions
1.	What is the self-perceived *role and function* of SRIA in the private sector?	(S14): In your experience, what is the main role and function of the SRIA in the private sector? (Open-ended format)
2.	Are there a shared self-perceived *uniqueness/esoteric "greater cause" to the* SRIA in the private sector?	(S15): In your experience, what is the unique contribution of SRIA to the private sector and to society? (Open-ended format)
3.	How do intelligence analysts, individually and collectively, conceptualise or define their professional identity?	S16): Please rate the extent to which you agree with each of the following statements: (S16/1) Generally, the more my goals, values, and beliefs overlap with those of my profession, the happier I am. (S16/2) I would rather say 'we' than 'they' when talking about the profession I work in. (S16/3) I strongly define myself as a security risk intelligence analysis professional. (S16/4) I'm not interested in what others think about the security risk intelligence analysis profession.* (S16/5) I currently attend /would like to attend events where security risk intelligence analysis best practice is shared. (S16/6) When someone praises the security risk intelligence analysis profession, it feels like a personal compliment. (S16/7) If a story in the media criticized the security risk intelligence analysis profession, I would feel embarrassed, e.g. the case of Reality Winner (link) (S16/8) All other factors being equal, I would rather change my employer than my profession as a security risk intelligence analyst. (S16/9) It is more important that I conduct my work professionally than being a member of a specific "profession". Likert scale: Strongly agree/Agree/Neither agree or disagree/disagree/strongly disagree * Reverse coding
4.	What is their perception of Security Risk Intelligence Analysis in the private sector?	(S17) : Please rate the extent to which you agree with each of the following statements: (S17/1) I think highly of the Security Risk Intelligence Analysis profession. (S17/2) I consider it prestigious to belong to the Security Risk Intelligence Analysis profession. (S17/3) I consider the Security Risk Intelligence Analysis profession to be one of the best professions for people with relevant skills and education. (S17/4) I would not recommend this career to someone else.*

	Research questions	Survey Questions
		(S17/5) I see a future for myself being a Security Risk Intelligence Analyst in the private sector and would like to remain in this profession in some capacity. Likert scale: Strongly agree/Agree/Neither agree or disagree/disagree/strongly disagree* Reverse coding
		(S24) In light of the fast-changing working environment, what skills do you think SRIA need to acquire to be relevant in the future? (Open-ended format)
5.	What experiences and conditions does SRIA perceive as contributing to or strengthening their professional identities?	(S18): What benefits/opportunities do you derive from you being a security risk intelligence analyst? Name at least 2. (Open-ended format)
6.	What experiences and conditions does SRIA perceive as hindering their professional identity?	(S19): In your experience, what are the biggest challenges you experience/d as a security risk intelligence analyst? (at least 2) (Open-ended format)
7.	How do SRIA believe they are perceived by others? 7.1 What is the public's viewpoint about the profession?	(S20): Please rate the extent to which you agree with each of the following statements: Likert scale: Strongly agree/Agree/Neither agree or disagree/disagree/strongly disagree *Reverse coding (S20/1): People, in general, think highly of the security risk intelligence analysis profession (S20/2): It is considered prestigious to belong to the security risk intelligence analysis profession. (S20/3): The security risk intelligence analysis profession is considered to be one of the best professions.
	7.2 How do your colleagues view your work and your contribution to the team?	(S20/4): Most of the stakeholders with whom I liaise value the contribution I, as a security risk intelligence analyst, make to achieve our mandate.
	7.3 How do your management and/or clients perceive you in your professional capacity?	(S20/5): My management and/or clients do not have a good perception of the profession of the security risk intelligence analyst. *
8.	What are the most salient professional values that SRIA share?	(S21): In your experience, what are the three most important/ non-negotiable professional values/ethical standards or codes of conduct that you practise as a Security Risk Intelligence Analyst? (Open-ended format)
9.	How do they perceive the future of the profession, and what should be done to ensure the profession stay relevant?	(S22) In your opinion, what would help to strengthen the identity of the Security Risk Intelligence Analysis profession for the future? (optional) (Open-ended format)

Collective Professional Identity Research Instrument Design

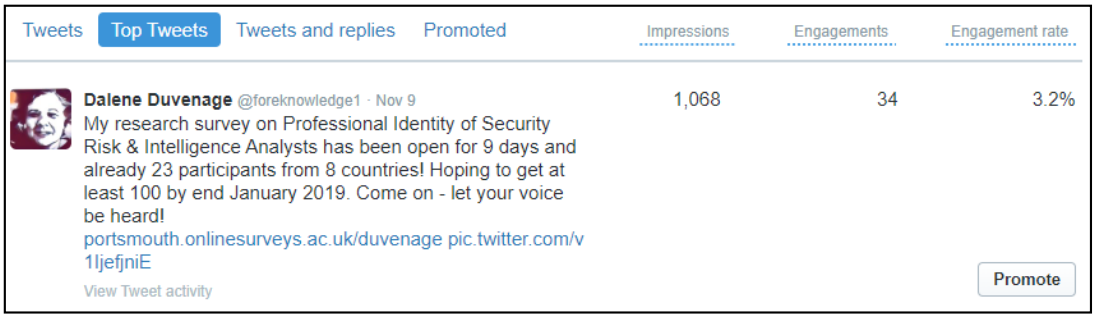
Appendix C3



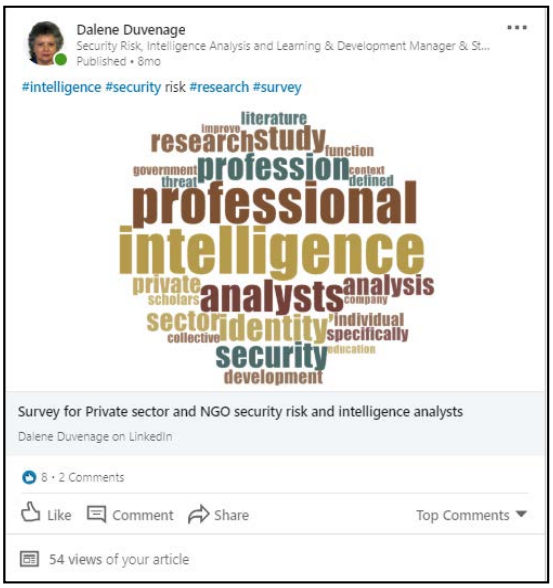
APPENDIX C4

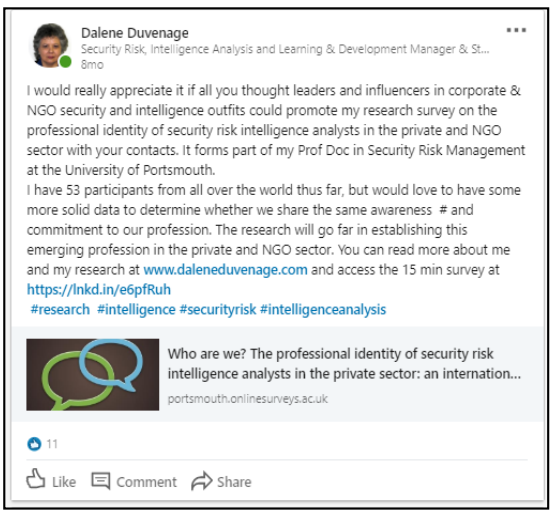
Social media marketing

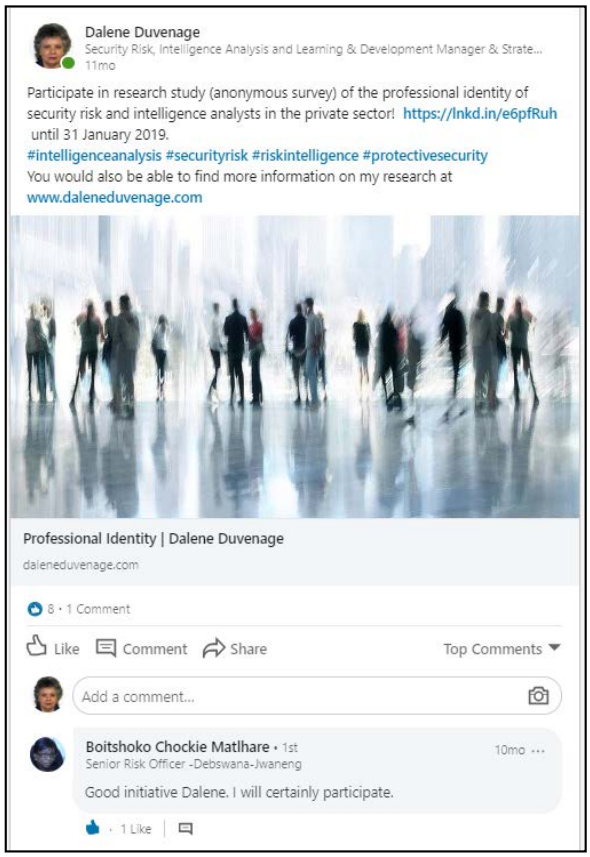
Screen shots of Twitter marketing of the survey



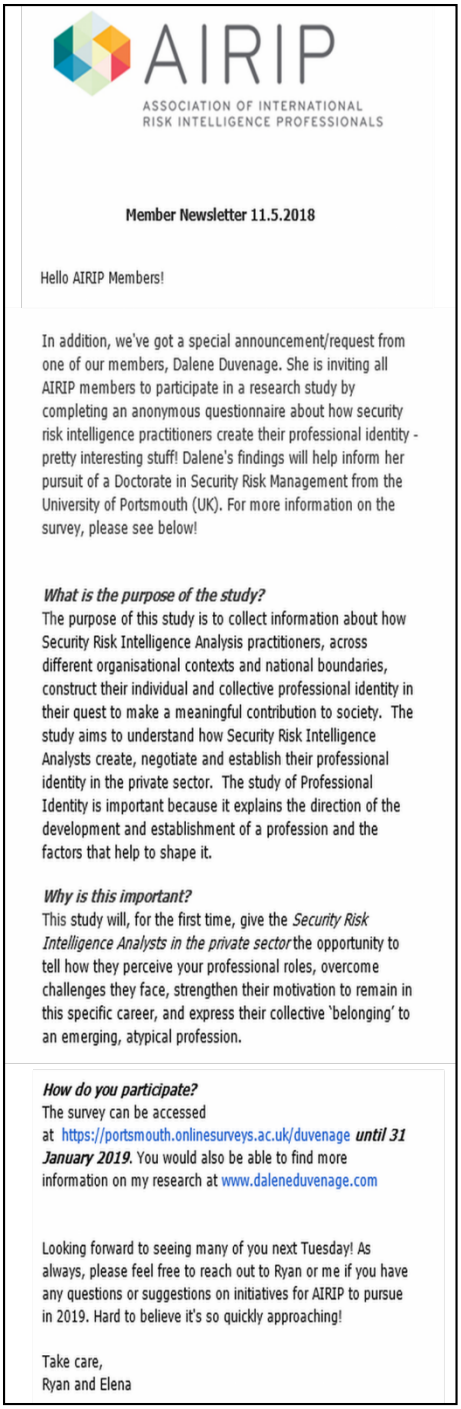
Screen shots of marketing of survey on LinkedIn social media network







Screenshot of AIRIP email to members (extract)



AIRIP

ASSOCIATION OF INTERNATIONAL RISK INTELLIGENCE PROFESSIONALS

Member Newsletter 11.5.2018

Hello AIRIP Members!

In addition, we've got a special announcement/request from one of our members, Dalene Duvenage. She is inviting all AIRIP members to participate in a research study by completing an anonymous questionnaire about how security risk intelligence practitioners create their professional identity - pretty interesting stuff! Dalene's findings will help inform her pursuit of a Doctorate in Security Risk Management from the University of Portsmouth (UK). For more information on the survey, please see below!

What is the purpose of the study?
The purpose of this study is to collect information about how Security Risk Intelligence Analysis practitioners, across different organisational contexts and national boundaries, construct their individual and collective professional identity in their quest to make a meaningful contribution to society. The study aims to understand how Security Risk Intelligence Analysts create, negotiate and establish their professional identity in the private sector. The study of Professional Identity is important because it explains the direction of the development and establishment of a profession and the factors that help to shape it.

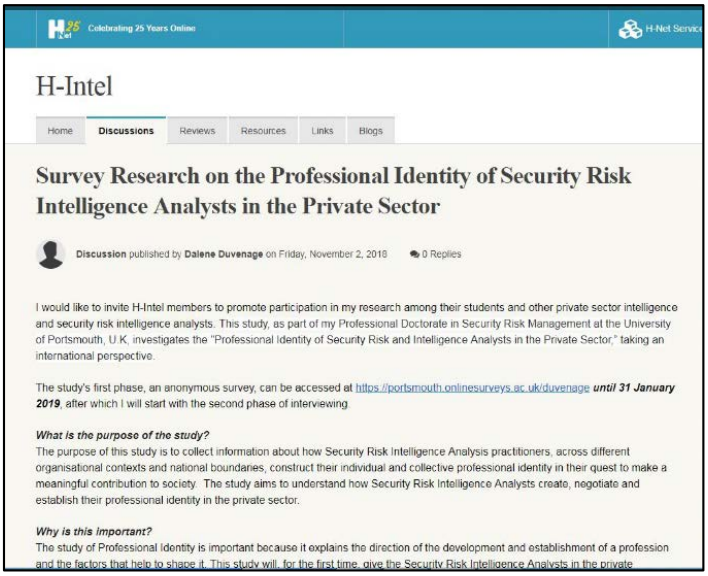
Why is this important?
This study will, for the first time, give the *Security Risk Intelligence Analysts in the private sector* the opportunity to tell how they perceive your professional roles, overcome challenges they face, strengthen their motivation to remain in this specific career, and express their collective 'belonging' to an emerging, atypical profession.

How do you participate?
The survey can be accessed at https://portsmouth.onlinesurveys.ac.uk/duvenage ***until 31 January 2019***. You would also be able to find more information on my research at www.daleneduvenage.com

Looking forward to seeing many of you next Tuesday! As always, please feel free to reach out to Ryan or me if you have any questions or suggestions on initiatives for AIRIP to pursue in 2019. Hard to believe it's so quickly approaching!

Take care,
Ryan and Elena

Screenshot of International Association for Intelligence Education (IAFIE) email to members (extract)



Celebrating 25 Years Online

H-Net Service

H-Intel

Home | Discussions | Reviews | Resources | Links | Blogs

Survey Research on the Professional Identity of Security Risk Intelligence Analysts in the Private Sector

Discussion published by **Dalene Duvenage** on Friday, November 2, 2018 0 Replies

I would like to invite H-Intel members to promote participation in my research among their students and other private sector intelligence and security risk intelligence analysts. This study, as part of my Professional Doctorate in Security Risk Management at the University of Portsmouth, U.K. investigates the "Professional Identity of Security Risk and Intelligence Analysts in the Private Sector," taking an international perspective.

The study's first phase, an anonymous survey, can be accessed at https://portsmouth.onlinesurveys.ac.uk/duvenage ***until 31 January 2019***, after which I will start with the second phase of interviewing.

What is the purpose of the study?
The purpose of this study is to collect information about how Security Risk Intelligence Analysis practitioners, across different organisational contexts and national boundaries, construct their individual and collective professional identity in their quest to make a meaningful contribution to society. The study aims to understand how Security Risk Intelligence Analysts create, negotiate and establish their professional identity in the private sector.

Why is this important?
The study of Professional Identity is important because it explains the direction of the development and establishment of a profession and the factors that help to shape it. This study will, for the first time, give the Security Risk Intelligence Analysts in the private

APPENDIX C5

SPSS Codebook for use in Mann-Whitney and Kruskal Willis tes*ts*

Variable	SPSS Variable name	Coding instructions
Unique response number	ID	
Age	Age	1= 18-24; 2= 25-34; 3= 35-44; 4= 45-54; 5= 55-65 6= 65+
Gender	Gender	1= Male; 2= Female
Years of SRIA experience	Yearsexperience	1= 1-5 years; 2= 6-10 years; 3= 11-15 years; 4= 16-20 years; 5= 21-25 years; 6= More than 25 years
Previous government experience	Previousgov	1 = Yes; 2 = No
Country in which you are working	Countryworking	1 = Australia; 2 = Botswana; 3 = Bulgaria; 4 = Canada; 5 = Finland ;6 = Germany; 7 = Global; 8 = Greece; 9 = Kenya; 10 = Lebanon ;11 = Mexico; 12 = Netherlands; 13 = Nigeria; 14 = Singapore; 15 = Slovenia; 16 = South Africa; 17 = Switzerland; 18 = Tanzania; 19 = UK; 20 = Ukraine; 21 = US; 22 = Venezuela
Supervisory position	Supervisor	1 = Yes; 2 = No
Economic sector	Sector	1 = Agriculture; 2 = Mining & Quarrying; 3 = Manufacturing; 4 = Electricity, Gas, Steam and Air Conditioning; 5 = Wholesale and Retail trade; repair of vehicles; 6 = Transport & Storage; 7 = Accommodation and Food service; 8 = Information & Communication; 9 = Finance & Insurance; 10 = Professional, Scientific & Technical; 11 = Public Sector, Social Security & Defence; 12 = Education; 13 = Human Health & Social Work; 14 = Arts, Entertainment & Recreation; 15 = Extraterritorial Organisations & Bodies
Type of organisation you're working for	Typeoforg	1 = Self-employed; 2 = A security/intelligence/risk unit in a private company/multinational corporation whose core business is not security 3 = A private security company with its own security risk intelligence analysis capacity. 4 = A private local/national/multinational company that provide security risk intelligence consulting services to external clients, including the private sector or government agencies. This would, therefore, also include contractors

Variable	SPSS Variable name	Coding instructions
		working in situ at Government departments/agencies. 5 = A non-governmental organisation (NGO) with its own security risk intelligence analysis capacity 6 = Research institute/foundations/think tanks whose primary function is to provide security risk intelligence analysis and advice to external clients. 7 = Independent regulatory/supervisory body.
Highest qualification	Qualification	1 = 1 or 2 year qualification 2 = Bachelors degree (3/4 years) or equivalent 3 = Honours degree (1yr after Bachelors) or equivalent 4 = Masters degree 5 = Doctorate degree
Field of qualification	QualField	1 = Education 2 = Arts and humanities including languages 3 = Social sciences, journalism and information, including Economics, political sciences, psychology, sociology 4 = Business, administration and law, including accounting, management, finance etc 5 = Natural sciences, mathematics and statistics 6 = Information and Communication Technologies (ICTs) 7 = Services including security, military, law enforcement 8 = Do not want to disclose
Membership of professional organisation	Professionalorg	1 = Yes 2 = No
Self-categorisation: Generally, the more my goals, values, and beliefs overlap with those of my profession, the happier I am.	SCValues	1 = Strongly agree 2 = Agree 3 = Neither agree nor disagree 4 = Disagree 5 = Strongly disagree
Self-categorisation: I would rather say 'we' than 'they' when talking about the profession I work in.	SCSaywe	
Self-categorisation: I strongly define myself as a Security Risk Intelligence Analysis professional.	SCIdefine	1 = Strongly agree 2 = Agree 3 = Neither agree nor disagree 4 = Disagree 5 = Strongly disagree
Self-categorisation: I'm interested in what others	SCOthers	

Variable	SPSS Variable name	Coding instructions
think about the Security Risk Intelligence Analysis profession.		
Self-categorisation: I currently attend /would like to attend events where Security Risk Intelligence Analysis best practice is shared.	SCEvents	
Self-categorisation: When someone praises the Security Risk Intelligence Analysis profession, it feels like a personal compliment.	SCCompliment	
Self-categorisation: If a story in the media criticized the Security Risk Intelligence Analysis profession, I would feel embarrassed, e.g. the case of Reality Winner, a US intelligence analysis contractor who was sentenced to jail in June 2018 after she leaked information to the media.	SCEmbarrassed	
Self-categorisation: All other factors being equal, I would rather change my employer than my profession as a Security risk intelligence analyst.	SCChange	
Self-categorisation: It is more important that I conduct my work professionally than being a member of a specific “profession".	SCProfessional	
The sum of the SC variables	TotalSelfcat	
Mean of each case’s responses	MeanTSelfcat	1 = Strongly agree 2 = Agree 3 = Neither agree nor disagree 4 = Disagree 5 = Strongly disagree
Self-perception: I think highly of the Security Risk Intelligence Analysis profession.	SPThinkhighly	
Self-perception: I consider it prestigious to belong to the Security Risk Intelligence Analysis profession.	SPPrestigious	
Self-perception: I consider the Security Risk Intelligence Analysis profession to be one of the best professions for	SPBest	1 = Strongly agree 2 = Agree 3 = Neither agree nor disagree 4 = Disagree

Variable	SPSS Variable name	Coding instructions
people with relevant skills and education.		5 = Strongly disagree
Self-perception: I would recommend this career to someone else.	SPRecommend	
Self-perception: I see a future for myself being a Security Risk Intelligence Analysis in the private sector and would like to remain in this profession in some capacity.	SPFuture	
Mean of each case's responses	MeanSelfpercep tion	
Others' perception: People, in general, think highly of the Security Risk Intelligence Analysis profession.	OPThinkhighly	
Others' perception: It is considered prestigious to belong to the Security Risk Intelligence Analysis profession	OPPrestigious	
Others' perception: The Security Risk Intelligence Analysis profession is considered to be one of the best professions.	OPBest	
Others' perception: Most of the stakeholders with whom I liaise value the contribution I, as a Security risk intelligence analyst, make to achieve our mandate.	OPValue	
Others' perception: My management and/or clients have a good perception of the profession of Security Risk Intelligence Analysis.	OPPerception	
Mean of each case's responses	MeanOthers	

APPENDIX C6

Operational definitions of themes for content analysis in the survey

Theme	Definition
Role and function of a security risk intelligence analyst	
Specific and varied roles of a security risk intelligence analyst	Any reference to one or more of the specific professional roles a security risk intelligence analyst fulfils.
Focus on the anticipatory role of intelligence analysis	Any reference to forewarning and intelligence function.
Focus on the insight role of intelligence analysis	Any reference to situational awareness & identification of threats and risks.
Whom SRIA work with	Any reference to the setting or breadth of settings SRIA work in or range of presenting problems addressed.
Use of typical jargon used by security, risk and/or intelligence analysts	Use of typical terminology and/or jargon used by security, risk or intelligence professionals in this role.
The unique contribution of a security risk intelligence analyst	
What SRIA offer the client in terms of better decision-making	Any reference to the interpersonal aspect of the security risk intelligence analyst role, including how they may help the client.
The perceived contribution to society	Any reference to esoteric and value-laden terminology to describe the contribution to society.
Use of specific risk prevention terminology that benefits the organisation	Any reference to the preventative aspect of the business.
Opportunities or benefits offered by working as a Security risk intelligence analyst Career	
Career and other physical personal outcomes	Any reference to one or more of the various career and personal opportunities working as a security risk intelligence analyst presents.
Own evaluation on how they feel about the profession.	Any comment on how they feel or experience being in this profession, the importance and/or enjoyment they derive from practising.
How others view the profession and how it impacts their own self-image	Any reference to how others view their contribution and how it impacts their self-image.
Challenges experienced whilst working as a Security risk intelligence analyst	
Organisational-situated challenges (outward facing)	Any comment highlighting the challenge of gaining recognition, understanding, resources, cooperation etc. in the workplace.
Challenges that originate from the task and function itself (inward-facing)	Any comment highlighting challenges specific to the security risk intelligence analysis task itself.
Challenges with the operational environment	Any comment highlighting challenges in the broader environmental/political context.
Challenges in the professional context not previously mentioned	Any comment highlighting tensions they experience within the professionalisation project itself.
Strategies that could strengthen the professional identity of SRIA	
Clearer articulation of identity and potential contribution to	Any comment highlighting the need for a clearer and more active promotion of the identity and potential contribution of SRIA.

organisation, cross-functional bodies and society	
Improved HR practices	Any comment highlighting ways in which SRIA could ensure that HR practices, such as job profiling, recruitment etc., could be improved.
Enhance the role of professional bodies and the profession	Any comment highlighting the need for a higher profile, greater recognition and increased networking within the professional bodies.
Training, education and research activity	Any comment relating to ways in which the training, education and researching of SRIA could improve the professional identity of analysts.
Self-awareness and ethical behaviour	Any comment highlighting the profession's need for a more positive self-perception or potential ways of achieving this.

Appendix C7

Survey results

Appendix C7.1

Table 1

Gender, age and experience distribution: n=75

Gender	18-24 years old	25-34 years old	35-44 years old	45-54 years old	55-65 years old	65+ years old	Total
Female	1	4	7	3	3	0	18
Male	1	11	14	16	13	2	57
Total	2	15	21	19	16	2	75

	1-5 years experience	6-10 years experience	11-15 years experience	16-20 years experience	21-25 years experience	> 25 years experience	Total
Female	3	2	4	6	0	3	18
Male	10	10	10	8	8	11	57
Total	13	12	14	14	8	14	75

Survey results

Appendix C7.2

Table 2
Field of qualification and highest qualification achieved: n=75

Answer options	1/2 year qualification	Bachelor's degree	Honours degree*	Master's degree	Doctorate degree	Total
Arts and humanities, including languages		3		5		8
Business, administration and law, including accounting, management, finance etc.		1	1	3	3	8
Do not want to disclose	1	2				3
Education		2	1	2	1	6
Information and Communication Technologies (ICTs)				3	1	4
Natural sciences, mathematics and statistics	1	2				3
Services including security, military, law enforcement		2	1	8		11
Social sciences, journalism and information including economics, political sciences, psychology, sociology	1	3	5	20	3	32
TOTAL	3	15	8	41	8	75

Note. In some countries, including the UK, Australia and South Africa, Honours degrees are one-year specialism qualifications awarded after the first (Bachelor's) degree and before the Master's degree.

Survey results

Appendix C7.3

Table 3

Economic sector and countries in which the analysts work: n=75

Answer options	Response %	Frequency	Countries
Accommodation and Foodservice	3%	2	USA
Agriculture	3%	2	South Africa, USA
Arts, Entertainment & Recreation	1%	1	USA
Education	5%	4	Greece, USA
Electricity, Gas, Steam and Air Conditioning	7%	5	Germany, Netherlands, USA
Extraterritorial Organisations & Bodies	1%	1	South Africa
Finance & Insurance	13%	10	Slovenia, South Africa, Switzerland, UK, USA
Human Health & Social Work	7%	5	Kenya, Tanzania, USA, Venezuela
Information & Communication	7%	5	Bulgaria, Finland, South Africa, USA
Manufacturing	5%	4	Germany, USA
Mining & Quarrying	5%	4	Botswana, Mexico
Professional, Scientific & Technical	32%	24	Germany, globally, Nigeria, Singapore, South Africa, UK, Ukraine, USA
Public Sector, Social Security & Defence	3%	2	Canada, Lebanon
Transport & Storage	5%	4	Australia, Canada, UK, USA
Wholesale and Retail trade; repair of vehicles	3%	2	UK, USA
TOTAL	**100%**	**75**	

Survey results

Appendix C7.4

Table 4

Type of employer and countries in which they are employed: n=75

Answer options	Response %	Frequency	Countries
A security/ intelligence/ risk unit in a private company/multinational corporation or university whose core business is *not* security.	47%	35	Australia, Botswana, Bulgaria, Canada, China, Germany, Korea, Mexico, Singapore, Slovenia, South Africa, Taiwan, UK, US, Venezuela
A private local/national/multinational company that provides security risk intelligence consulting services to external clients, including the private sector or government agencies. This would, therefore, also include contractors working in situ at government departments/agencies.	16%	12	Australia, Finland, Netherlands, South Africa, UK, US
A private security company with its own security risk intelligence analysis capacity.	13%	10	Nigeria, Ukraine, US
Self-employed	12%	9	Germany, South Africa, US & 2X global
A non-governmental organisation (NGO) with its own security risk intelligence analysis capacity.	8%	6	Kenya, Lebanon, Switzerland, Tanzania, US
Research institute/foundations/think tanks whose primary function is to provide security risk intelligence analysis and advice to external clients.	3%	2	Greece and South Africa
Independent regulatory/supervisory body.	1%	1	Canada
TOTAL	100%	75	

Survey results

Appendix C7.5

Table 5
Focus areas of analytical services and deliverables: n=75

Answer options	Response %	Frequency
Analytical practices		
Strategic analysis & Foresight	64%	48
Analytical practices	37%	28
Mean of respondents	51%	38
Security management		
Security risk management	71%	53
Security management strategy	55%	41
Physical protection of facilities	48%	36
Strategic security management	39%	29
Governance and/or compliance	36%	27
Business continuity/crisis management	3%	2
Mean of respondents	42%	31
Protective/security intelligence		
Travel risk	57%	43
Personnel security incidents	51%	38
Reputational risks	51%	38
Executive protection	40%	30
Insider threats	40%	30
Loss prevention	35%	26
Internal investigations	31%	23
Fixated/psychological disturbed persons of interest	16%	12
Mean of respondents	**40%**	**30**
Geostrategic & political intelligence		
Geo-political developments	63%	47
Terrorism & counter-terrorism	53%	40
Extremism	49%	37
National political developments	44%	33
Political economy developments	35%	26
Espionage threats	33%	25
Socio-economic developments	33%	25
Military threats	23%	17
Interest and pressure groups	21%	16
Mean of respondents	**39%**	**30**
Crime intelligence		
General crime	59%	44
Organised crime	49%	37
Environmental crime/risks	41%	31

Answer options	Response %	Frequency
Corruption	31%	23
Money laundering and fraud	21%	16
Terrorist financing	9%	7
Mean of respondents	**35%**	**26**
Cyber intelligence		
Cyber threats	24%	18
Cyber threat analysis	23%	17
Mean of respondents	**24%**	**18**

Survey results

Appendix C7.6

Table 6

Membership of professional organisations, gender and reasons for belonging to a professional organisation: n=52

Answer options	Response %	Frequency
Member of a professional organisation	72%	52
Male	71%	40
Female	75%	12
Age Groups		
18-24	100%	2
25-34	60%	9
35-44	65%	13
45-54	78%	14
55-64	80%	12
65+	100%	2
Reasons for being a member of a professional organisation		
Networking & socialising	34%	33
Information sharing/Staying informed/Access to opportunities	20%	19
Benchmarking/best practice	18%	17
Learning/professional development	18%	17
Certification/professional recognition specifically	8%	8
Company requires it	2%	2
NOT member of a professional organisation	26%	19
Male	27%	15
Female	25%	4
Age Groups		
18-24	0%	0
25-34	40%	6
35-44	35%	7
45-54	17%	3
55-64	20%	3
65+	0%	0
Reasons for NOT belonging to a professional organisation		
No need for it	53%	10
Lack of awareness	26%	5
Cost	16%	3

Survey results

Appendix C7.7

Table 7

Professional organisation membership and qualification comparison

Answer options	% who belong to prof organisations	Frequency *n*=52	Mean number of prof memberships of *all* participants with qualifications
1 or 2 year qualification	67%	2	1.3
Bachelor's degree (3/4 years) or equivalent	53%	8	1.4
Honours' degree (1yr after Bachelors) or equivalent	63%	5	0.9
Master's degree	78%	32	1.9
Doctorate degree	63%	5	1.8

Survey results

Appendix C7.8

Table 8

Professional organisational type 1: Membership of professional organisations that provide networking, knowledge sharing AND professional certification opportunities n=20

Answer options	Response %	Frequency
Prof Org with certification options & knowledge sharing according to membership frequency		
Association for International Risk Intelligence Professionals (AIRIP)	26%	14
ASIS (formerly American Society of Industrial Security)	26%	14
Security Institute	11%	6
Association for certified Fraud Examiners (ACFE)	9%	5
Association of Threat Assessment Professionals (ATAP)	9%	5
Business Continuity Institute (BCI)	4%	2
International Association of Crime Analysts (IACA)	4%	2
International Security Management Institute (ISMI)	4%	2
International NGO Safety and Security Association (INSSA)	2%	1
ACM (formerly Association for Computing Machinery)	2%	1
AOC (Association of Old Crows - a professional organization that advocates the technical advancement of Electronic Warfare and Information Operations)	2%	1
Chartered Insurance Institute (CII)	2%	1
Chartered Society of Forensic Science (CSFS)	2%	1
Disaster Recovery Institute International (DRII)	2%	1
EC-Council (International Council of E-Commerce Consultants)	2%	1
Global Business Travel Association - GBTA	2%	1
International Association of Computer Investigative Specialists (IACIS)	2%	1
International Association of Emergency Managers (IAEM)	2%	1
International Association for Law Enforcement Intelligence Analysts	2%	1
International Supply Chain Protection Organization (ISCPO)	2%	1
ACM (formerly Association for Computing Machinery)	2%	1
AOC (Association of Old Crows - a professional organization that advocates the technical advancement of Electronic Warfare and Information Operations)	2%	1
Chartered Insurance Institute (CII)	2%	1
Chartered Society of Forensic Science (CSFS)	2%	1
Disaster Recovery Institute International (DRII)	2%	1

Survey results

Appendix C7.9

Table 9

Professional organisation Type 2: Membership of professional organisations that provide networking, knowledge sharing with a code of conduct or professional standards, but no professional certification: n=23

Answer options	Response %	Frequency
Professional organisation without certification options		
OSAC (Overseas Security Advisory Council - a division of the U.S. Department of State's Bureau of Diplomatic Security)	17%	9
Analyst Roundtable (ad hoc workshops of experts/analysts that are industry/professional organization/geography specific)	15%	8
Private Sector Intelligence Council (PSIC)	6%	3
AFIO (Association for Intelligence Officers)	4%	2
AIIP (Association of Independent Information Professionals)	4%	2
Domestic Security Alliance Council (DSAC)	4%	2
International Association for Intelligence Education (IAFIE)	4%	2
ISC2 International Information Systems Security Certification Consortium	4%	2
Asian Crisis Security Group (ACSG)	2%	1
Business Resumption Planners Association (BRPA)	2%	1
Electronic Crimes Task Force	2%	1
PULSE: Higher Education International Health and Safety Professionals (Canada and US)	2%	1
High Technology Crime Investigation Association (HTCIA) US & Canada)	2%	1
Institute of Electrical and Electronics Engineers (IEEE)	2%	1
Institute of Information Technology Professionals of South Africa (IITPSA)	2%	1
Infragard (US)	2%	1
International Protective Security Board (IPSB)	2%	1
International Studies Association (ISA)	2%	1
NAFSA (Started as National Association of Foreign Student Advisers) now Association of International Educators	2%	1
National Efficiency Screening Project (NESP)	2%	1
National Military Intelligence Association (NMIA)	2%	1
Strategic and Competitive Intelligence Professionals (SCIP)	2%	1
University Risk Management and Insurance Association	2%	1

Survey results

Appendix C7.10

Table 10
The perceived benefits of belonging to the security risk intelligence analysis profession: n=73

Themes and sub-themes	% of respondents whose answers included a code in the theme	% of countries whose answers included a code in the theme: *n*=24	% of economic sectors whose answers included a code in the theme: *n*=15
Personal benefits	**83%**	**73%**	**93%**
Intellectually stimulating career	51%	54%	73%
Good self-esteem	14%	21%	53%
Networking opportunities	13%	17%	40%
Other (no need for security clearance, access to databases, etc.)	11%	13%	53%
Flexibility and travel opportunities	10%	13%	33%
Good salary	7%	17%	20%
Perceived image of the profession inside and outside the professional group (validation)	**17%**	**29%**	**53%**
Valued by peers	8%	15%	40%
Valued by management and executives	6%	20%	27%
Valued by clients	1%	10%	13%
Self-perceived value of them belonging to the profession	**32%**	**38%**	**73%**
They have an impact on the business	14%	22%	53%
Serving others / Making a difference	11%	17%	27%
Impact on profession	4%	13%	13%

Survey results

Appendix C7.11

Table 11

The perceived challenges associated with being a security risk intelligence analyst profession: n=71

Themes and sub-themes	% of respondents whose answers included a code in the theme	% of countries whose answers included a code in the theme: *n*=24	% of economic sectors whose answers included a code in the theme *n*=15
1. **Challenges related to their task**	**39%**	**38%**	**80%**
1.1 Information and cognitive overload	24%	25%	60%
1.2 Cognitive biases and challenges	8%	8%	20%
1.3 Time pressure	7%	13%	33%
1.4 Difficult to influence decision makers	6%	8%	13%
1.5 Lack of feedback	1%	4%	7%
2. **Challenges stemming from organisational context**	**80%**	**92%**	**93%**
2.1 Lack of understanding the value of security risk intelligence analysis	54%	67%	80%
2.2 Lack of resources	27%	25%	60%
• Lack of access to information	13%	17%	33%
• Lack of funding	14%	25%	47%
• Lack of IT resources	4%	8%	20%
2.3 Inadequate HR support	23%	33%	60%
• Lack of career pathing	8%	17%	53%
• Uninformed recruiters and poor recruitment practices	14%	25%	33%
2.4 Training challenges	11%	25%	40%
2.5 Lack of interdepartmental cooperation and information sharing	11%	8%	40%
• With external stakeholders	3%	4%	13%
• With internal stakeholders	8%	8%	33%
2.6 Inadequate salary	6%	13%	20%
2.7 Age and gender bias	3%	13%	20%
2.8 Politicization	1%	4%	7%
3. **Challenges in the operating environment (rapid geopolitical changes and the role of artificial intelligence to assist with information gathering)**	**14%**	**17%**	**53%**
4. **Challenges in the broader profession (lack of networking, the profession is unknown, few opportunities in the industry etc.)**	**3%**	**8%**	**13%**

Appendix C7.12

Table 12

The most important/non-negotiable professional values/ethical standards or codes of conduct that you practise as a Security risk intelligence analyst: n=71

Themes and sub-themes	% of respondents whose answers included a code in the theme	% of countries whose answers included a code in the theme: *n*=24	% of economic sectors whose answers included a code in the theme: *n*=15
1. Personal values	**80%**	**83%**	**73%**
1.1 Integrity	52%	58%	100%
1.2 Honesty	42%	46%	73%
1.3 Learning disposition	11%	13%	27%
1.4 Courage	10%	13%	33%
1.5 Lawful	8%	21%	40%
2. Values related to how they perform their task	**72%**	**83%**	**73%**
2.1 Objective	34%	50%	67%
2.2 Discretion	28%	46%	73%
2.3 Strive for excellence	20%	25%	53%
2.4 Collaborate	10%	8%	20%
2.5 Customer-centric	10%	13%	27%
2.6 Ethical data gathering	7%	8%	20%
3. Values related to their organisation	**10%**	**25%**	**33%**
3.1 Managers support analysts' judgements	3%	8%	13%
3.2 Independence	3%	8%	13%
3.3 Loyalty	3%	8%	13%
Values related to how they interact with others	10%	17%	27%
4.1 Respect	6%	13%	20%
4.2 Professional	4%	8%	13%

Survey results

Appendix C7.13

Table 13

Self-identification/categorisation with the security risk intelligence analyst profession

Answer options	1: Strongly agree n (%)	2: Agree n (%)	3: Neither agree nor disagree n (%)	4: Disagree n (%)	5: Strongly disagree n (%)	Mean/SD
1) Generally, the more my goals, values, and beliefs overlap with those of my profession, the happier I am.	39 (52%)	25 (33%)	9 (12%)	2 (3%)	0 (0%)	1.65/0.79
2) I would rather say 'we' than 'they' when talking about the profession I work in.	43 (57%)	27 (36%)	5 (7%)	0 (0%)	0 (0%)	1.49/0.62
3) I strongly define myself as a SRIA professional.	27 (36%)	24 (32%)	15 (20%)	8 (11%)	1 (1%)	2.09/1.05
4) I'm not interested in what others think about the SRIA profession.*	3 (4%)	3 (4%)	13 (17%)	32 (43%)	24 (32%)	3.92/1.0
5) I currently attend /would like to attend events where SRIA best practice is shared.	49 (65%)	23 (31%)	2 (3%)	1 (1%)	0 (0%)	1.4/0.61
6) When someone praises the SRIA profession, it feels like a personal compliment.	23 (31%)	22 (29%)	25 (33%)	4 (5%)	1 (1%)	2.17/0.97
7) If a story in the media criticized the SRIA profession, I would feel embarrassed, e.g. the case of Reality Winner.	12 (16%)	13 (17%)	26 (35%)	15 (20%)	8 (11%)	2.92/1.21
8) All other factors being equal, I would rather change my employer than my profession as a SRIA.	31 (41%)	18 (24%)	12 (16%)	12 (16%)	2 (3%)	2.15/1.2
9) It is more important that I conduct my work professionally than being a member of a specific "profession".	42 (56%)	23 (31%)	8 (11%)	2 (3%)	0 (0%)	1.6/ 0.78
OVERALL RESULTS	**43%**	**31%**	**17%**	**7%**	**2%**	**1.95/0.91**

* Reverse coding

Appendix C7.14

Table 14

Results of Mann-Whitney (U test) and Kruskal-Wallis (H Test) nonparametric tests across demographic variables: Self-categorisation

Dependent variable	Gender	Age Group	Years' experience	Organisation type	Economic Sector	Country working	Previous gov experience	Managemen t position	Profess org member	Qualification
Generally, the more my goals, values, and beliefs overlap with those of my profession, the happier I am. (SCValues)	Similar distributio n U=415 p =.180	Similar distributio n H=2.852 p =.723	Similar distributio n H=5.722 p =.334	Similar distributio n H=3.214 p =.782	Similar distributio n H=15.868 p =.321	Similar distributio n H=20.382 p =.497	Similar distributio n U=529, p=234	Similar distributio n U=586.5, p=.749	Similar distributio n U=545.5, p =.506	Similar distributio n H=2.848 p =.584
I would rather say 'we' than 'they' when talking about the profession I work in. (SCSaywe)	Similar distributio n U=400 p=.109	Similar distributio n H=1.445 p =.919	Similar distributio n H=1.537 p =.909	Similar distributio n H=3.746 p =.711	Similar distributio n H=7.241 p =.926	Similar distributio n H=24.265 p =.280	Similar distributio n U=591, p =.662	Similar distributio n U=493, p=.122	Similar distributio n U=549, p =.520	Similar distributio n H=4.182 p =382
I strongly define myself as a Security Risk Intelligence Analysis professional. (SCIdefine)	Similar distributio n U=334 p=.013	Similar distributio n H=.662 p =.987	Similar distributio n H=2.763 p =.736	Similar distributio n H=8.459 p =.206	Similar distributio n H=8.535 p =.860	Similar distributio n H=20.512 P=.489	Similar distributio n U=601, p=.0778	Similar distributio n U=573.5, p=.647	Similar distributio n U=584.5, p =.871	Similar distributio n H=3.733 p =.443

Dependent variable	Gender	Age Group	Years' experience	Organisation type	Economic Sector	Country working	Previous gov experience	Management position	Profess org member	Qualification
I'm interested in what others think about the Security Risk Intelligence Analysis profession (SCOthers)	Similar distribution U=499.5 p=.060	Similar distribution H=3.969 p =.554	Similar distribution H=5.281 p =.383	Similar distribution H=3.718 p =.715	Similar distribution H=14.997 p =.378	Similar distribution H=16.559 p =.737	Similar distribution U=623, p =.981	Similar distribution U=521, p=.272	Similar distribution U=540, p =.479	Similar distribution H=5.929 p =.205

I currently attend /would like to attend events where Security Risk Intelligence Analysis best practice is shared.(SCEvents)	Similar distribution U=507.5 p=.935	Similar distribution H=9.142 p =.104	Similar distribution H=3.300 p =.654	Similar distribution H=3.718 p =.715	Significantly different distribution H=28.565 p=.012 Mean ranks in order of positive to negative: Agriculture, Mining, Finance, Public sector, Health=25; Professional=37; Info & Comm=39.40; Manufacturing, Retail =43; Electricity =53.8; Education =55.5;Arts	Similar distribution H=20.104 p =.515	Significantly different distribution U=444 p =.014 Mean ranks: Yes: 41.62 No: 30.76	Similar distribution U=564 p =.512	Similar distribution U=595 p =.967	Similar distribution H=4.353 p =.360

Dependent variable	Gender	Age Group	Years' experience	Organisation type	Economic Sector	Country working	Previous gov experience	Management position	Profess org member	Qualification
					etc, Extraterritorial bodies=61, Accommodation=67.2					
When someone praises the Security Risk Intelligence Analysis profession, it feels like a personal compliment. (SCompliment)	Similar distribution U=512.500 p =.995	Similar distribution H=1.726 P=.886	Similar distribution H=3.150 p =.677	Similar distribution H=5.280 p =.508	Similar distribution H=11.530 p =.644	Similar distribution H=20.342 p =.500	Similar distribution U=614 p =.901	Similar distribution U=580 p =.703	Similar distribution U=495 p =.214	Similar distribution H=4.287 p =.369
If a story in the media criticized the Security Risk Intelligence Analysis profession, I would feel embarrassed (SCEmbarrassed)	Similar distribution U=432.5 p=.304	Similar distribution H=1.982 P=.852	Similar distribution H=7.593 p =.180	Similar distribution H=2.346 p =.885	Similar distribution H=6.476 p =.953	Similar distribution H=32.613 p =.051	Similar distribution U=571 p =.532	Significantly different Distribution U=412 p =.020 Mean ranks: Yes: 34.09 No: 46.31	Similar distribution U=581 p =.845	Similar distribution H=1.878 p =.758

Dependent variable	Gender	Age Group	Years' experience	Organisation type	Economic Sector	Country working	Previous gov experience	Management position	Profess org member	Qualification
All other factors being equal, I would rather change my employer than my profession as a Security risk intelligence analyst. (SCChange)	Similar distribution U=334 p=.401	Similar distribution H=3.039 P=.694	Similar distribution H=6.461 p =.264	Similar distribution H=4.600 p =.596	Similar distribution H=17.885 p =.212	Similar distribution H=15.446 p =.800	Similar distribution U=619 p =.944	Similar distribution U=458 p=.066	Similar distribution U=558.5 p =.634	Similar distribution H=6.875 p =.143
It is more important that I conduct my work professionally than being a member of a specific "profession". (SCProfessional)	Significantly different Distribution U=334 p =.013 Mean ranks: Male: 34.86 Females: 47.94	Similar distribution H=6.177 P=.289	Similar distribution H=3.623 p =.605	Similar distribution H=9.896 p =.129	Similar distribution H=18.111 p =.202	Similar distribution H=15.183 p =.814	Similar distribution U=3568.5 p=.476	Significantly different Distribution U=443 p =.031 Mean ranks: Yes: 34.69 No: 45.04	Similar distribution U=461.5 p =.078	Similar distribution H=2.445 p =.655

Appendix C7.15

Table 15

Results of Mann-Whitney (U test) and Kruskal-Wallis (H Test) nonparametric tests across demographic variables: Collective Self-perception

Dependent variable	Gender	Age Group	Years' experience	Organisation type	Economic Sector	Country working	Previous gov experience	Management position	Profess org member	Qualification
think highly of the Security Risk Intelligence Analysis profession. (SPThinkhighly)	Similar distribution U=463.5, p=.498	Similar distribution H=4.686 p=.455	Similar distribution H=3.680 p =.596	Similar distribution H=3.567 p =.735	Similar distribution H=18.845 p =.171	Similar distribution H=17.391 p =.687	Similar distribution U=580 p =.577	Similar distribution U=513 p =.215	Similar distribution U=521.5 p =.332	Similar distribution H=3.070 p =.546
I consider it prestigious to belong to the Security Risk Intelligence Analysis profession. (SPPrestigious)	Similar distribution U=480.500, p=.671	Similar distribution H=8.929 p=.112	Similar distribution H=6.998 p =.221	Similar distribution H=2.940 p =.861	Similar distribution H=20.192 p =.124	Similar distribution H=27.862 p =.144	Similar distribution U=607 p =.831	Similar distribution U=518 p =.261	Similar distribution U=561.5 p =.659	Similar distribution H=3.894 p =.421
I consider the Security Risk Intelligence Analysis profession to be one of the	Similar distribution U=475.5 p=.618	Similar distribution H=4.850 p=.434	Significantly different distribution H=11.712 p =.039	Similar distribution H=7.912 p =.245	Significantly different distribution H=27.352 p =.017	Similar distribution H=30.084 p =.090	Similar distribution U=615 p =.904	Significantly different Distribution U=442 p =.039	Similar distribution U=485.5 p =.166	Similar distribution H=1.442 p =.837

best professions for people with relevant skills and education. (SPBest)			Mean ranks: 1-5 years: 46.08 6-10 years: 35.92 11-15 years: 26.04 16-20 years: 32.46 21-25 years:40.81 25+ years: 48.18		Mean ranks in order of positive to negative: Agriculture & Mining=10.5; Health=16; Finance=32.5; Public sector=36.75; Education=37.38; Info& comm=37.5 Arts & Extraterritorial org=38; Transport=39.88 Professional=44.04; Manufacturing=44.25; Wholesale=50.5; Electricity=55;			Mean ranks: Yes: 34.67 No: 45.08		

					Accommodation=63					
I would recommend this career to someone else. (SPRecommend)	Similar distribution U=449.5 p=.398	Similar distribution H=1.697 p=.889	Similar distribution H=7.922 p =.161	Similar distribution H=5.313 p =504	Similar distribution H=6.015 p =.966	Similar distribution H=28.799 p =.139	Similar distribution U=593 p=.700	Similar distribution U=468 p =.080	Similar distribution U=553 p =.579	Similar distribution H=3.960 p =.411
I see a future for myself being a Security Risk Intelligence Analysis in the private sector and would like to remain in this profession in some capacity. (SPFuture)	Similar distribution U=425 p =.244	Similar distribution H=1.563 p=906	Similar distribution H=1.626 p =.898	Similar distribution H=4.506 p =.609	Similar distribution H=19.932 p =.132	Similar distribution H=18.259 p =.633	Similar distribution U=588.5 p=.662	Similar distribution U= 520 p =.265	Similar distribution U=535 p =.440	Similar distribution H=5.599 p =.231

Survey results
Appendix C7.16

Table 16

Results of Mann-Whitney (U test) and Kruskal-Wallis (H Test) nonparametric tests across demographic variables: Collective perception of others

Collective perception of others' perceive the security risk intelligence analysis profession					
Dependent variable	People in general think highly of the SRIA profession (OPThinkhighly)	It is considered prestigious to belong to the SRIA profession (OPPrestigious	The SRIA profession is considered to be one of the best professions (OPBest)	Most of the stakeholders with whom I liaise value the contribution that I, as a SRIA, make to achieve our mandate (OPValue)	My management/ clients have a good perception of the SRIA profession (OPPerception)
Gender	Similar distribution U=414 p =.188	Similar distribution U=505 p =.915	Similar distribution U=411 p =.173	Similar distribution U=471 p =.559	Similar distribution U=465 p =534
Age Group	Significantly different distribution H=11.580 p =.041 Mean ranks: 18-24: 10 25-34: 30.33 35-44: 39.10 45-54: 42.47 55-65: 38.06 65+ : 69.00	Similar distribution H=1.563 p=906	Similar distribution H=1.563 p=906	Similar distribution H=1.563 p=906	Similar distribution H=1.563 p=906
Years' experience	Similar distribution H=6.718 p =.242	Similar distribution H=8.166 p =.147	Similar distribution H=5.179 p =.394	Similar distribution H=.521 p =.991	Similar distribution H=4.018 p =.547
Organisation type	Similar distribution H=6.130 p =.409	Similar distribution H=5.500 p =.481	Similar distribution H=10.456 p =.107	Similar distribution H=2.636 p =.853	Similar distribution H=4.505 p =.609
Economic Sector	Similar distribution H=19.245 p =.156	Similar distribution H=7.746 p =.902	Similar distribution H=16.173 p =.303	Similar distribution H=9.506 p =.797	Similar distribution H=14.175 p =.437
Country working	Similar distribution H=26.799 p =.178	Similar distribution H=20.776 p =.473	Similar distribution H=19.859 p =.530	Similar distribution H=10.212 p =.976	Similar distribution H=19.289 p =.567
Previous gov experience	Similar distribution U=564 p=.462	Similar distribution U=509.500 p=.163	Similar distribution U=593 p=.698	Similar distribution U=618 p=.930	Similar distribution U=558.5 p=.430
Management position	Similar distribution U=564 p =.559	Similar distribution U=544.5 p =410	Similar distribution U=467.50, p =.077	Similar distribution U=563 p =.533	Similar distribution U=490.5 p =.149
Profess org member	Similar distribution U=580 p =.824	Similar distribution U=541.5 p =.485	Similar distribution U=527.5 p =.383	Similar distribution U=556 p =.589	Similar distribution U=540.5 p =.490
Qualification	Similar distribution H=3.885 p =.422	Similar distribution H=3.151 p =.533	Similar distribution H=7.056 p =.133	Similar distribution H=.411 p =.982	Similar distribution H=3.711 p =.447

Appendix D1

Interview information sheet

Institute of Criminal Justice Studies
University of Portsmouth
St George's Building, 141 High Street
Portsmouth PO1 2HY
Email:magdalena.duvenage@myport.ac.uk
1 November 2018

Dear participant

Prof Doc Research on the Professional Identity of Security Risk Intelligence Analysts in the Private Sector: an International Perspective

You are invited to participate in a research study on the above topic, which I am undertaking as part of my Professional Doctorate in Security Risk Management at the University of Portsmouth, UK.

The study aims to understand how Security Risk Intelligence Analysts create, negotiate and establish their professional identity in the private sector. The study of Professional Identity is important because it explains the direction of the development and establishment of a profession and the factors that help to shape it.

The ideal participants in the study would be analysts who are currently working in the private or non-governmental organisation (NGO) sector with the job titles of security risk or threat analyst, crime analyst, crime intelligence analyst, research specialist, political risk analyst, cyber threat analyst, intelligence manager, security risk manager etc.

I am seeking 8 to 12 interviewees who would be willing to participate in a telephone or Skype interview of approximately 45 minutes. Any calling costs will be borne by myself. Interviews will be completely anonymous and confidential, and the anonymity of you, and your organisation will be preserved. The interview will be recorded digitally. Based on this recording a transcript will be generated. Participants will be permitted to withdraw from the research at any time prior to the analysis of the data.

Included with this letter is an information sheet that explains more about the research and its processes. Also included is a consent form, which you will be asked to return if you are willing to participate in the research. I very much hope you will be interested in participating.

Should you have any specific queries or concerns please feel free to contact me (magdalena.duvenage@myport.ac.uk), or my research supervisor, Dr Moufida Sadok (moufida.sadok@port.ac.uk).

I would be grateful if you could confirm with me via my email address above if you are willing to take part in the research.

MA (Dalene) Duvenage

Institute of Criminal Justice Studies
University of Portsmouth
St George's Building, 141 High Street
Portsmouth PO1 2HY
Email:magdalena.duvenage@myport.ac.uk
Date: 1 November 2018

PARTICIPANT INFORMATION SHEET

Title of Project:	**Who are we? The professional identity of security risk intelligence analysts in the private sector: an international perspective**
Name and Contact Details of Researcher:	Dalene Duvenage Email: magdalena.duvenage@myport.ac.uk
Name and Contact Details of Supervisor:	Dr Moufida Sadok Email: moufida.sadok@port.ac.uk

1. Invitation

I would like to invite you to take part in my research study on the professional identity of Security Risk Intelligence Analysts in the private sector. Joining the study is entirely up to you, but before you decide, I would like you to understand why the research is being done and what it would involve for you. I will go through this information sheet with you, to help you decide whether or not you would like to take part and answer any questions you may have. I would suggest this should take about 45 minutes. Please feel free to talk to others about the study if you wish. Do ask if anything is unclear.

I am a Candidate for the Professional Doctorate in Security Risk Management at the University of Portsmouth in the UK and have about 30 years of experience in the security risk and intelligence analysis field in South Africa.

2. Study Summary

This study will, for the first time, give the Security Risk Intelligence Analysis (SRIA) profession in the private sector across various countries, the opportunity to tell how they perceive their professional roles, overcome challenges they face, strengthen their motivation to remain in this specific career, and express their collective 'belonging' to an emerging, atypical profession.

The ideal participants in the study would be analysts who are currently working in the private or non-governmental organisation (NGO) sector with the job titles of security risk or threat analyst, crime analyst, crime intelligence analyst, research specialist, political risk analyst, cyber threat analyst, intelligence manager, security risk manager etc. They should have access to a telephone, Skype or WhatsApp voice/video call facility for the interviews. Their place of employment should be outside the government, and more specifically they should be employed by any of the following:

- a private security company with its own security risk analysis capacity;

- a security/intelligence/risk unit in a company/multinational corporation whose core business is not security;
- a private company which provides security risk and threat intelligence consulting services to external clients, including the private sector or government agencies. This would therefor also include contractors working in situ at government departments/agencies;
- A non-governmental organisation with its own security risk analysis capacity;
- An intergovernmental organisation with its own security risk analysis capacity or
- A researcher in the academia/institutions/foundations/think tanks whose primary function is to provide security risk analysis and advice to external clients.

3. What is the purpose of the study?

The study aims to understand how Security Risk Intelligence Analysts create, negotiate and establish their professional identity in the private sector. The study of Professional Identity is important because it explains the direction of the development and establishment of a profession and the factors that help to shape it.

The study entails the use of two sequential research instruments. The first was a web-based survey which will run between November 2018 and January 2019. The second is these in-depth semi-structured Skype of telephonic interviews with a number of security risk intelligence analysts across different employment and national contexts who have indicated in the survey that they want to be interviewed.

The results of the research will determine whether there is a shared individual and collective professional identity. The interview should not take longer than 30-45 minutes on average and could be done whenever it suits the interviewee the best.

4. Do I have to take part?

No, taking part in this research is entirely voluntary. It is up to you to decide if you want to volunteer for the study. I will describe the study in this information sheet. If you agree to take part, I will then ask you to sign the attached consent form, dated 1 November 2018.

5. What will happen to me if I take part?

The interview should last approximately 45 minutes, using the mode of communication that you indicated in our communication after the survey. The Skype interview will start with some general questions to understand your demographic background after which I will ask questions that will not be invasive or deal with sensitive aspects of your career. The interviews will be recorded for transcription later. All identifying information will be replaced with pseudonyms to ensure anonymity. I will also share the transcription of the interview with you so that you can inform me if there you want to change something, or even if you want to withdraw from the study. The transcriptions will then be analysed using Interpretative Phenomenological Analysis which allows the researcher to obtain nuanced, rich information on the lived experience of the individuals.

6. Expenses and payments

Please take note that the researcher will carry the expenses with regard to the telephone or Skype interview, but your country's telecommunications services might deduct additional fees from your account. Please take this into account when indicating your willingness to participate.

7. Anything else I will have to do?

No, there is nothing else you need to do after the interview, unless you want to peruse the transcription of your interview for your final approval.

8. What data will be collected and / or measurements taken?

The data collected will mainly be about your experiences and perspectives about being a security risk intelligence analyst in the private sector. No propriety or sensitive "need-to-know" data will be collected. Opinions and statements made during the interview might be referenced or quoted within the thesis or relevant academic journals. However, your identity will be safeguarded with the preservation of your anonymity and your organisation. You will not be expected to disclose any information that may be sensitive, and every effort will be made to remove any specific details which could allow your employer or yourself to be identified.

9. What are the possible disadvantages, burdens and risks of taking part?

There should be no disadvantages for participating in this research as no intimate or personal data will be collected.

11. What are the possible advantages or benefits of taking part?

The main benefit for you personally might be that this is the first time that you are given the opportunity to be reflective about your profession and how you perceive it. This would increase your self-knowledge and your future in this profession.

12. Will my taking part in the study be kept confidential?

Yes, absolutely. The raw data, which identifies you, will be kept securely by the researcher and the university and will be password protected. Confidentiality will be kept, unless you tell me that you don't mind me using your first name in the research. Otherwise, your name will be changed to some generic name in the discussion of the results. All records will be changed so that the generic/anonymous name is used. The data, when made anonymous, may be presented to others at academic conferences, or published as a thesis, academic journals or book. A CC-BY licence will be applied to this publicly shared data. This will allow anyone else (including researchers, businesses, governments, charities, and the general public) to use the anonymised data for any purpose that they wish, providing they credit the University and research team as the original creators. No restrictions will be placed on this shared anonymised data limiting its reuse to only non-commercial ventures.

The recordings of the interviews will be similarly kept in a password protected folder with only the researcher having access and on request; the supervisor might gain access during the finalisation of the thesis. The audio recordings will be destroyed soon after collection when the data for analysis have been extracted.

The raw data, which would identify you, will not be passed to anyone outside the study team without your express written permission. The exception to this will be any regulatory authority which has the legal right to access the data for the purposes of conducting an audit or enquiry, in exceptional cases. These agencies treat your personal data in confidence.

The raw data will be retained for a minimum of 10 years as per the records management policies of the University of Portsmouth. When it is no longer required, the data will be disposed of securely (*e.g.* electronic media and paper records / images) destroyed.

13. What will happen if I don't want to carry on with the study?

As a volunteer you can stop any participation in the interview at any time, or withdraw from the study up to two weeks after the interview, without giving a reason if you do not wish to. If you prefer, the data collected can be destroyed and not included in the study. You can also review the transcript for accuracy or to withdraw any particular comments which you do not want to appear in the public domain. However, once the research has been completed, and the data analysed, it will not be possible for you to withdraw your data from the study.

14. What if there is a problem?

If you have a query, concern or complaint about any aspect of this study, in the first instance you should contact the researcher(s) or the supervisor with details of the complaint. The contact details for both the researcher and any supervisor are detailed on page 1.

If your concern or complaint is not resolved by the researcher or their supervisor, you should contact the Head of Department:

The Head of Department	Dr Paul Norman
Institute of Criminal Justice Studies	023 9284 3459
University of Portsmouth	paul.norman@port.ac.uk

If the complaint remains unresolved, please contact:

The University Complaints Officer 023 9284 3642 complaintsadvice@port.ac.uk

15. Who is funding the research?

The study is not funded and the researcher will not receive any financial reward by conducting this study, other than her salary and bursary from her employer.

16. Who has reviewed the study?

Research involving human participants is reviewed by an ethics committee to ensure that the dignity and well-being of participants is respected. This study has been reviewed by the ICJS Faculty Ethics Committee and been given favourable ethical opinion.

Thank you

Thank you for taking time to read this information sheet and for considering participating for this research. If you do agree to participate, you will need to complete the accompanying consent form. You will then be given a copy of this information sheet and your signed consent form.

Appendix D2

Research journal

Date	Reflections
19/07/2020	I realised that I had to use the research questions as my compass, as my lack of a psychological background and insights could lead me astray from the pertinent points that I had to investigate. I would easily become engrossed in, for instance, the elements of job satisfaction, while it was not a main element of my research objectives.
	I know I have to bracket between cases, but when I see similarities with previous case, it should be OK to acknowledge it and then try to counter it?
18/07/2020	I had a look again at how other scholars did their theming, I went through my lit review to get an idea (so the theory got stuck, so what? This is not trying to find a cure for Covid19, is it?
	As I go through other people's themes, I struggle to find the connection with their research objectives. It feel as though it have been written down as with a shopping list. So to what extent do I keep my research questions in my thesis in line with the transcript?
	Murphy: What are these things that makes it easier to develop and maintain a PI? In SRIA this is till absent: 1) a shared ideology of work (we have that, I'm showing it now with this study) What is "act like"? To have a 2) prototype, - a collective understanding of who constitutes the ideal member o this profession, with curriculum and standardised role.(to build prototype of previous gov intel experience and then start new hybrid profession that newcomers then emulate?) 3) Image transparency (external perception)
17/07/2020	I struggle to bracket my usual analytical, summarising mind
	Re Liz's interview: to what extent does personal growth (growing out of a job or organisation) have o PI? When you have outgrown your current position and the organisation could not grow with you due to various org dynamics reasons – much like myself and SARB. I feel exhausted by analysing interview because it so sad and superficial. I thought I missed underlying issues, I put myself in her shoes to remember when I went through the same process of alienation and feeling that I outgrew my organisation. I remember the fear but also not knowing what is inside me and how to verbalise that what I am going through. There is just this multitude of feelings (warboel), but the overall one I had was that I'm not happy, and I need to get out, but economic realities just made it impossible. That defeatist's alienation and subsequent spiritual craziness that I'm not fulfilling my calling just made things very bad for me. At long last, now that I know about identity work, I have some framework to hang my experience on. I can give words to my memories and feelings.
16/07/2020	Re the interviews: I should have focused more on the identity crises and how the dealt with it than on what they're doing on a daily basis.
11/07/2020	To what extent did COVID19 change business' and the world's perception about Risk management, negative news, black hatters? War-mongers? Is this going to change the perceived need for us positively? The fact that we are now in the frontlines to protect? Keep track of new threats, hybrid threats. Therefor a new opportunity to expand responsibility and show our value. https://intelligence.weforum.org/topics/a1Gb0000001SG51EAG?tab=publications. Incorporation of security risk into whole of company risk management – more multidisciplinary teams. Protection now upfront in everyone's' minds. Combine SRM with OHS & supplier due diligence and cyber security

Appendix D3

Interview schedule

Demographic information:

Name
Age
Gender
Country of citizenship
In which country do you work?
Years' experience specific in this capacity?
Highest qualification:
Where have you worked previously?
Where do you work? What economic sector is that?
On what types of threats or issues do you work?
Are you a member of a professional organisation? Which? Why? Why not?

1. **What does it mean to you personally to be a SECURITY RISK INTELLIGENCE ANALYST in the private sector**?
   Prompts:
   - What are your responsibilities?
   - What do you do on a daily basis?
   - With whom do you work and why?
   - What is your official job title? Is this a true reflection of what you do? What would you prefer your job title to be?

2. **When people ask what you do for a living, what do you tell them? Tell me your professional story?**
   Prompts:
   - What or who got you into the security risk intelligence field?
   - How do you feel when you're working?

3. **Is there anything that the Security Risk Intelligence Analyst bring to the table that no-one else does?**
   Prompts:
   What makes this career different from any other career?

4. **What is that something special that you bring as a Security Risk Intelligence Analyst to your workplace? And the broader society?**

5. **What do you like about being a Security Risk Intelligence Analyst? Why?**
   Prompts:
   - What does it offer to you personally that no other career can?
   - What benefits are there for you?
   - Why does it make you feel good?
   - Is there a future for this career?
   - Would you recommend this career to anyone else?
   - Can anybody do this job?

6. **What experiences and conditions impede your Security Risk Intelligence Analyst professional identity?**
   Prompts:

- In your experience, what are the biggest challenges you experience/d as a Security Risk Intelligence Analyst?
- What do you dislike about being a Security Risk Intelligence Analyst?

7. **Did you ever feel you had a professional identity crisis? Can you share that with me?**
   Prompts:
   - What happened? What was the reason?
   - How did you overcome/are you overcoming these challenges?
   - Did you have to change the way you see yourself professionally?
   - Change your expectations?
   - Change the way you work?

8. **How do other people perceive you professionally?**
   Prompts:
   - Have you had experience with the public, and how do they perceive you in your professional role?
   - What about your colleagues?
   - Your managers?
   - Your clients?

9. **In your opinion, what would help to strengthen the identity of the Security Risk Intelligence Analysis profession for the future?**
   Prompts:
   - Skills & competencies
   - Relationships
   - Education and training
   - Socialising & networking
   - Professional associations & credentials?
   - Professional conduct
   - Values
   - Understand your role/place
   - Is there a professional community?

Thank you for your time and willingness to share your experiences.

Appendix D4

Consent form

Institute of Criminal Justice Studies
University of Portsmouth
St George's Building, 141 High Street
Portsmouth PO1 2HY
Email:magdalena.duvenage@myport.ac.uk
1 November 2018

CONSENT FORM

Title of Project: **Who are we? The professional identity of security risk intelligence analysts in the private sector: an international perspective**

Please initial

1. I have read and understood the invitation & information sheets dated 1 November 2018 about this study. I understand the purpose and nature of the research. ☐

2. I confirm of being aware that my participation is voluntary. I am satisfied that, prior to the data being analysed, I can withdraw my participation and permission for data usage at any time up to two weeks after completing the interview without any justification. ☐

3. I am fully aware that some of the collected data will be included in the thesis, journal articles and academic presentations under the condition of anonymity being maintained. I fully support use of data in publications for general access and on the University of Portsmouth library website, coupled with the fact that only the researcher and the research supervisor can access the original data. I also understand that the no other person will access the original data with destruction after completing analysis of the data. ☐

4. I agree to interviews being recorded for the purpose of conducting an IPA analysis based on this recording. ☐

5. I agree to take part in the above study. My employing organisation agrees with my participation in the above study. ☐

Name of participant: _____

Participant's signature: _____ Date _____

Name of researcher: Magdalena Adriana Duvenage

Researcher's signature: _____ Date _____

Should you have any specific queries or concerns please feel free to contact me (magdalena.duvenage@myport.ac.uk), or my research supervisor, Dr Moufida Sadok (moufida.sadok@port.ac.uk).

Appendix D5

Sample of interview transcript

Transcription of Skype interview with A on 28 February 2019 (page 8 of 18)

Demographics: Male, 38 years old, 16 years' experience, of which 10 years in Military and 6 years in private sector
Highest academic qualification: Bachelors
US, pharmaceutical company

Interviewer: ***When people with no knowledge of this field ask you what you're doing for a living what do you tell them?***

A: So I start with "I do research and analysis" because that's what I do: " in-depth research analysis on security related topics with a focus on anything that involves crime impacting the company". It's really where our bread and butter is, criminal impact on the company and that's what it is research analysis on that...

Interviewer: ***How do you feel when you are working? Do you like your job?***

A: Yeah, I mean I think you know, it's one of those … you know this community or this profession I think still in the private sector it's a little better …but it's kind of it's a very thankless kind of position right?
Because you're not in a leadership position and when things go wrong you're to blame, and when things go right, somebody else usually gets the credit. That's just how it is. But, I think if you're humble enough to understand that even though you've done a bulk of the work that the lead investigator may be briefing it, and you know, getting a lot of good feedback, you have to find, you know find satisfaction in that because that's the role they've chosen.
If you wanted to be a leader then you should have gone that route. I mean these people are better in a support infrastructure, support role and you have to understand the support role. I mean I think I've been in leadership positions but with the intelligence community but I always work for a commander or a leader or a director or supervisor. And I think I think if you can be humble enough it can be very satisfying. And you know, it's really hard work we're doing. And it's hard trying to stay on top of things, if you can persevere through the end result whether that's a good case you resolved or you've influenced a business decision.
If you have set good thresholds for what success is, so you know, what course of action or business makes a decision based on what you said - you know this little thing you can be humble enough. I think I would have worked hard over the years, you know I tried to get out of this position because it was thankless and I wasn't getting my credit. And I think it was, just you know you're young and you want to be the top.

Appendix E

UNIVERSITY OF PORTSMOUTH

Professional Identity worksheet

This sheet will help you to define your own professional identity, regardless of what work you do.

1. **Your name:**

2. **What is your preferred job title for the work you're doing?**

3. **What are the unique set of skills, character and attitude that you bring to your workplace?** (see further reading)

4. **Do you feel satisfied and fulfilled in your workplace, and why?**

5. **What are your 3 most important professional values?**

6. **What are the 3 things you like most about your job? What gives you energy, excitement or gratitude?**

7. **What are the 3 things that you dislike the most about your job? What saps your energy, what makes you irritable and what do you dread?**

8. **How do you deal with these 3 challenges? Choose the strategy/ies you use when confronted with these:**

- [ ] Resign from the job
- [ ] Become demotivated
- [ ] Alienate yourself from colleagues
- [ ] Marginalise (which include name-calling, rejection and hostility) those people you think are a threat to your professional identity
- [ ] Implement acts of resistance
- [ ] Make sure that you manipulate how others see you
- [ ] Craft your job by 1) changing the boundaries of your tasks or 2) changing the nature and extent of your interaction with people.*
- [ ] Do introspection and reframe your perceptions on the purpose of tasks or job as a whole.*
- [ ] Reinvent yourself by learning new skills to address competency gaps or perhaps start a new career that will make work meaningful to you.*

9. **How are you going to address the challenges by changing yourself and applying any of those* above?**

Further reading:

1. Berg, JM., Dutton, JE and Wrzesniewski, A., (2008) What is Job Crafting and Why Does It Matter? Here
2. Mindtools. Job Crafting: Shaping Your Job to Fit You Better. Here
3. Take the free character strengths survey here

Your personal professional identity statement

(to use in introductions, interviews, LinkedIn profile etc.)

Hi! I'm (your name)

I work as a (your preferred job title)

at (the organisation you work for)

My unique value proposition to and impact in the organisation/purpose) is: e.g. I help my company to understand the threats and security risks to our business by researching, monitoring and advising business units on how to identify and counter or mitigate these risks to achieve their objectives while keeping the company and our employees safe.

I believe in doing my work with (values)

I can use my qualification/s in …

and my experience in … to provide the best ... possible

I like working with/learning/doing… (your objectives you would like to achieve/opportunities you have or would like to have in a new job)